Avaya Call Management System

Software Installation, Maintenance, and Troubleshooting

Release 16.3
September 2014

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site:

http://www.avaya.com/support

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://www.avaya.com/support/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. 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 End User. "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. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, 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 Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Named User License (NU). Customer may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use 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 Product that permits one user to interface with the Product.

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://www.avaya.com/support/ThirdPartyLicense/

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 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 Web site:

http://www.avaya.com/support

Trademarks

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:

http://www.avaya.com/support

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Contents

Preface

Avaya Call Management System (CMS) is an application for businesses and organizations that use Avaya communication servers to process large volumes of telephone calls using the Automatic Call Distribution (ACD) feature. Avaya CMS supports solutions for routing and agent selection, multi-site contact centers, remote agents, reporting, interfaces to other systems, workforce management, desktop applications, system recovery, and quality monitoring.

Avaya CMS is part of the Operational Effectiveness solution of the Avaya Customer Interaction Suite.

This section includes the following topics:

- Purpose on page 11
- Intended users on page 11
- Overview on page 12
- Conventions and terminology on page 13
- Reasons for reissue on page 13
- Documentation Web sites on page 14
- Support on page 14

Purpose

The purpose of this document is to describe how to install, configure, and maintain Avaya CMS.

Intended users

This document is written for:

- Avaya support personnel.
- Avaya factory personnel.
- Contact center administrators.

Users of this document must be familiar with Avaya CMS and the Solaris operating system.

Overview

This document includes the following topics:

- Introduction on page 17

  Provides an overview of the supported Avaya CMS software, supported hardware platforms and required software.

- Setting up the Mirror Disk Volume on page 17

  Provides an overview of the steps required for mirroring CMS data. Mirroring introduces data redundancy which greatly reduces the risk of data loss in the event of a disk failure or system crash.

- Installing the Solaris operating system on page 19

  Outlines the Solaris operating system installation procedures. These procedures are used by technicians at customer sites and personnel at the factory.

- Configuring the Solaris operating system on page 49

  Outlines the Solaris operating system configuration procedures. These procedures are used by technicians at customer sites and personnel at the factory.

- Installing Avaya CMS and supporting software on page 61

  Outlines the Avaya CMS software installation and setup procedures. These procedures are used by technicians at customer sites and by personnel at the factory.

- Turning the system over to the customer on page 127

  Provides the procedures that a technician performs before turning the system over to the customer and a worksheet that the technician fills out for the customer.

- Maintaining the Avaya CMS software on page 141

  Discusses file system backups and other maintenance procedures.

- Recovering an Avaya CMS system on page 209

  Provides recovery procedures.

- Troubleshooting on page 237

  Discusses how to fix various software - related problems.

Conventions and terminology

If you see any of the following safety labels in this document, take careful of the information presented.

⚠ **CAUTION:**
Caution statements call attention to situations that can result in harm to software, loss of data, or an interruption in service.

⚠ **WARNING:**
Warning statements call attention to situations that can result in harm to hardware or equipment.

⚠ **DANGER:**
Danger statements call attention to situations that can result in harm to personnel.

⚠ **SECURITY ALERT:**
Security alert statements call attention to situations that can increase the potential for unauthorized use of a telecommunications system.

Reasons for reissue

This document includes the following update:

- Additional procedures for the Sun SPARC T4-1 platform.
- Support for LTO-5 tape drive.
- Addition of Perle UltraPort1 Express PCIe Serial Card for T4-1 platform.

Note:
Oracle Corporation now owns Sun Microsystems. Instead of rebranding references to Sun Microsystems with the Oracle name, all occurrences of Sun and Sun Microsystems will remain as is in this document.

- Changed caution note about Solaris patches installation.
- Information on CMS Security is now in document *CMS Security.*
- Changed caution note on page 164.
- Updated steps in section "Installing the Solaris patches".

July 2013

- Changed directory name for pkgadd command on page 57.

- Steps to determine how much dataspace is required for the CMS full maintenance backup.

November 2013

- Steps for installing Access Security Gateway.
- Steps for system firmware updates during spatches installation.

August 2014

- Changed the Linux and Solaris NFS Server configuration sections so that the owner and group are set to `nfsnobody` at the time of writing to the network mount point.
- Added section *Generating and installing a customer certificate for the cmsweb server.*

September 2014

- Added note to refrain from adding a hyphen to the host name because of third-party tools.

Documentation Web sites

All CMS documentation can be found at http://www.avaya.com/support. New issues of CMS documentation will be placed on this Web site when available.

Use the following Web sites to view related support documentation:

- Information about Avaya products and service

  http://www.avaya.com

- Sun hardware documentation

  http://docs.sun.com

Support

Contacting Avaya technical support

Avaya provides support telephone numbers for you to report problems or ask questions about your product.

For United States support:

1- 800- 242-2121

For international support:

See the 1-800 Support Directory listings on the Avaya Web site.

Escalating a technical support issue

Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Management listings on the Avaya Web site.

Introduction

This section lists the hardware platforms and software that is supported by Avaya Call Management System (CMS) Release 16.3 (R16.3).

This section includes the following topics:

- Prerequisites on page 17
- Supported hardware platforms on page 17
- Supported software packages on page 18

Prerequisites

Before you use any procedures in this document, perform the following tasks:

- Review the file called **cms.readme** on the Avaya CMS software disc. Avaya recommends you review this file for any changes that might impact the procedures in this document.
- Contact Provisioning by calling 1-800-242-2121 extension 69366. The CMS provisioners must be scheduled in advance for all work. Provisioning is required to authorize the following features on CMS:
  - CMS Agent licenses.
  - CMS Supervisor licenses.
  - Call History Interface
  - ACDs.
  - Report Designer.
  - Provisioning will also work with your on-site team to insure connectivity and data collection.

Supported hardware platforms

Avaya CMS is supported on the following platforms:

- Sun SPARC Enterprise T5120 4-core
- Sun SPARC Enterprise T5120 8-core

- Sun SPARC Enterprise T5220
- Sun Netra X4270
- Sun SPARC T4-1

Note:
Unless specified otherwise, all information and procedures in this document apply to all the supported Avaya CMS hardware platforms. For more information regarding installation, maintenance and troubleshooting of the above platforms, please refer to the respective *Hardware Installation, Maintenance and Troubleshooting* documents.

Supported software packages

Avaya CMS utilizes the following software packages:

- Informix SQL
- Informix IDS (includes ODBC/JDBC)
- Informix Client ESQL SDK
- Informix ILS
- AVAYA CMS Supplemental Services for this release
- Avaya CMS R16.3 Software Installation disc, also contains:
  - Sun Solaris patches
  - Avaya CMS patches
  - Avaya security script
- Avaya Visual Vectors Server Release 16 (optional)

Installing the Solaris operating system

This section contains procedures to guide you step by step through the Solaris software installation. The installation program also has on line help to answer your questions. Depending on your platform type, not all the installation screens described in this section will be displayed by your system. There are special instructions in a few places that are for specific platforms. Those are noted with "T5120/T5220 only", “T4-1 only” or "x86 only" before the instruction(s).

> ⚠ **Important:**
> If the software was installed at the factory, proceed to Installing Avaya CMS and supporting software on page 61.

To bring the Avaya Call Management System (CMS) up to factory standards after a system re-configuration or repair, use the procedures in this section and Installing Avaya CMS and supporting software on page 61.

This section includes the following topics:

- Required hardware on page 19
- Prerequisites on page 20
- Installing Solaris 10 on page 20
- Selecting the Solaris software packages on page 32
- Configuring the disk drives for T5120/T5220/x86 on page 43
- Completing the Solaris installation on page 48

Required hardware

This release of CMS utilizes RAID to mirror the system. Mirroring allows you to create two complete sets of data on separate disk drives. This data redundancy greatly reduces the risk of data loss in the event of a disk drive failure or a system crash.

The Avaya CMS system must have a RAID hardware controller installed before installing Solaris 10 and the Avaya CMS software. Refer to the platform related *Hardware Installation and Maintenance* document for instructions on how to install the RAID hardware controller.

> ⚠ **Important:**
> Configuring RAID on a system will cause all data to be lost. A CMSADM or LAN restore will be required to restore the system after mirroring has been configured.

Prerequisites

Before you begin the installation procedures, perform the following tasks:

- You must have the platform specific RAID hardware controller installed in the system.
- You must have the correct number of disk drives to mirror a system. All disks must be of the same size.
- Obtain the Solaris 10 SPARC or x86 software disc.
- Identify the host name of the system, which is designated by the Technical Service Center (TSC).
- Identify the Internet Protocol (IP) address of the system (this may be the factory default or an address in a customer's network).
- Identify the default router for the system (this may be the factory default or an address in a customer's network).
- Identify the subnet mask for the system (this may be the factory default or an address in a customer's network).
- Identify the number and size of disk drives on the system.
- Verify that all power cords are fully connected to all hardware devices, and that power is applied to all hardware devices.
- Identify the tape devices on the system.
- Verify that all hardware components of the system, including port cards, external disk drives, and tape drives, are correctly installed.

Installing Solaris 10

This section describes the booting procedure for SPARC and x86 systems.

- If installing Solaris 10 on a T5120 or T5220, continue with Booting a T5120/T5220 system to the Solaris 10 DVD on page 21.
- If installing Solaris 10 on a Netra X4270, continue with Booting an x86 system to the Solaris 10 DVD on page 25.
- If installing Solaris 10 on a T4-1, continue with Booting a T4-1 system to the Solaris 10 DVD on page 23.

Booting a T5120/T5220 system to the Solaris 10 DVD

Important:
Use this procedure for the T5120 and T5220 platforms only.

This procedure is for booting the system from the Solaris software disc using the local console.

1. Verify the correct number of hard drives are inserted for your platform.
   - If the platform is a T5120 4-core, the system must have disks installed in slots 0, 1, 2 and 3.
   - If the platform is a T5220 or T5120 8-core, the system must have disks installed in slots 0, 1, 2, 3, 4 and 5.
2. Disconnect all USB storage devices.
3. Turn on the power to all of the external devices, such as tape drives.
4. Turn on the monitor.
5. Power on the Avaya CMS system.

Note:
Depending on the model, it can take several minutes for the system to boot up.

6. As the console shows that the system is booting up, press **Stop+A.**

   The system displays an ok prompt.
7. Set auto-boot? to **false**, enter:

   ```
   setenv auto-boot? false
   ```
8. In some cases the system will not boot from the cdrom if the eeprom variable `fcode-debug`? is not set to true. Make a note of the current `fcode-debug`? value before changing the value. To set the eeprom variable `fcode-debug`? to true, enter:

   ```
   setenv fcode-debug? true
   ```
9. The system needs to be reset before the `probe-scsi-all` command is executed to detect the hardware controller and disks. At the `ok` prompt enter:

   ```
   reset-all
   ```

   The screen will turn black. It could take up to 2 minutes for the system to reset and the `ok` prompt to be displayed.
10. Execute the `probe-scsi-all` command to detect the hardware configuration. At the `ok` prompt enter:

    ```
    probe-scsi-all
    ```

    Press **Enter.**

Important:
If prompted, press Enter to accept the current configuration.

The system displays messages associated with the Hardware Controller starting and the detection of scsi devices on the screen.

- If the system responds with messages similar to "Waiting for AAC Controller to start ………..Started", you have an AAC RAID controller. Continue with Step 11.
- If the system does not respond with messages similar to "Waiting for AAC Controller to start ………..Started". Continue with Step 12.

11. Check for any error messages:
    - If the system does not display any error messages after accepting the current configuration, continue with Step 14.
    - If a CRITICAL ERROR message is displayed after accepting the current configuration perform the following steps:
        a. Power off the system, enter:

           `power-off`

        b. Repeat Step 3 through Step 10. If the error occurs again, escalate through normal channels.
12. Wait for the system to display the `ok` prompt.
13. At the ok prompt, enter `show-disks` as shown in the example. If the output has an option containing "`LSI,mrsas@0`", you have an MRSAS RAID adapter. Continue with Step 14.

```
show-disks
a) /pci@0/pci@0/pci@9/LSI,mrsas@0/disk
b) /pci@0/pci@0/pci@8/pci@0/pci@9/pci@0/scsi@8,1/disk
c) /pci@0/pci@0/pci@8/pci@0/pci@9/pci@0/scsi@8/disk
d) /pci@0/pci@0/pci@2/scsi@0/disk
e) /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@2/disk
f) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit:
```

    Enter **q**.

14. Insert the Solaris 10 SPARC software disc into the disc drive.

    Important:
    If the system is being restored, be sure to insert the same version of Solaris that was used to build the original CMS system.

15. Boot to the Solaris 10 DVD, enter

    `boot cdrom`

16. The system boots from the disc and displays a list of languages.
17. Select the language that is appropriate for your location, and press Enter.

    The system displays "**Welcome**" Screen.

Note:
Do not select **Next**.

18. Continue with Configuring RAID on page 26.

Booting a T4-1 system to the Solaris 10 DVD

⚠ **Important:**
Use this procedure for the T4-1 platform only.

This procedure is for booting the system from the Solaris software disc using the local console.

1. Verify the correct number of hard drives are inserted for your platform. The system must have disks installed in slots 0, 1, 2, 3, 4 and 5.
2. Disconnect all USB storage devices.
3. Turn on the power to all of the external devices, such as tape drives.
4. Turn on the monitor.
5. Power on the Avaya CMS system.

Note:
It can take several minutes for the system to boot up.

6. When the console shows that the system is booting up, press **Stop+A**.

   The system displays an ok prompt.

7. Set `auto-boot`? to false, enter:

   ```
   setenv auto-boot? false
   ```

8. In some cases, the system will not boot from the cdrom if the eeprom variable `fcode-debug`? is not set to true. Make a note of the current `fcode-debug`? value before changing the value. To set the eeprom variable `fcode-debug`? to true, enter:

   ```
   setenv fcode-debug? true
   ```

9. The system needs to be reset before the `probe-scsi-all` command is executed to detect the hardware controller and disks. At the **ok** prompt enter:

   ```
   reset-all
   ```

   The screen turns black. It could take up to 2 minutes for the system to reset and display the **ok** prompt.

10. Execute the `probe-scsi-all` command to detect the hardware configuration. At the **ok** prompt enter:

    `probe-scsi-all`

    Press **Enter**.

11. Check for any error messages:

    - If the system does not display any error messages, continue with Step 14.
    - If the system displays a CRITICAL ERROR message, perform the following steps:

      a. Power off the system, enter:

         `power-off`

      b. Repeat Step 3 through Step 10. If the error occurs again, escalate through normal channels.

12. Wait for the system to display the **ok** prompt.

13. At the **ok** prompt, enter `show-disks` as shown in the example. The output should have an option containing "`LSI,mrsas@0`", indicating a MRSAS RAID adapter is present. Continue with Step 14.

```
show-disks
a) /pci@400/pci@2/pci@0/pci@f/pci@0/usb@0,2/hub@2/hub@3/storage@2/disk
b) /pic@400/pci@2/pci@0/pci@c/LSI,mrsas@0/disk
c) /pci@400/pci@2/pci@0/pci@4/scsi@0/disk
d) /pci@400/pci@1/pci@0/pci@4/scsi@0/disk
e) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit:
```

14. Insert the Solaris 10 SPARC software disc into the disc drive.

    ⚠ **Important:**
    If the system is being restored, be sure to insert the same version of Solaris that was used to build the original CMS system.

15. Boot to the Solaris 10 DVD, enter:

    `boot cdrom -sw`

16. The system boots from the disc and displays a list of languages.

17. The system displays "SINGLE USER MODE" and the # prompt.

18. Continue with Configuring RAID on page 26.

Booting an x86 system to the Solaris 10 DVD

Important:
Use this procedure for the x86 platform only.

This procedure is for booting the system from the Solaris software disc using the local console.

Prior to installing Solaris on the x86 system, you must set the boot priority.

1. Verify disks are installed in slots 0 and 1.
2. Disconnect all USB storage devices.
3. Turn on the power to all of the external devices, such as tape drives.
4. Turn on the monitor.
5. Power on the Avaya CMS system.

   As the system boots, the system displays a series of messages to the screen. One of the options listed in the American Megatrends screen is to "Press F2 to setup BIOS". Begin pressing the **F2** key when the system displays the American Megatrends screen.
6. Press **F2**.

   Note:
   The user may need to press the **F2** key many times before the selection is recognized. Continue to press the **F2** key even while additional installation information is displayed to the screen. The system does not display the BIOS Setup screen until after the system device information is displayed.

   - If the system displays the BIOS screen, continue with Step 7.
   - If the system does not display the BIOS screen, press `Ctrl+Alt+Del` and repeat Step 6 until the BIOS screen is displayed.
7. Press the right arrow key until you get to the "**Boot**" option in the upper BIOS menu.
8. Press the down arrow key until you reach "**Boot Device Priority**".

   Press **Enter**.
9. Verify that the CD/DVD drive is the first option in the boot order and the RAID volume is second. The network devices should be disabled for boot. Make the necessary changes to configure the system boot options as described.
10. Press the **F10** key to save and exit. Select **<OK>**. Press **Enter**.
11. Insert the Solaris 10 x86 software disc is in the disc drive, enter:

    ```
    Ctrl+Alt+Del
    ```

    Note:
    If the system appears to hang then manually power off the system and manually power the system back on.

    The system boots from the Solaris 10 x86 software disc.

12. Select "Solaris" at the **Grub** screen.

    The system displays a series of dots during the boot process. When the system is finished configuring the devices, it displays a list of options along with a warning stating that the user has 30 seconds to respond.

13. Enter the number associated with the **Solaris Interactive(default)** option.

    The system displays a series of messages while it attempts to configure the network interfaces, set up Java, and then begins the Extracting windowing system process.

    The **Configure Keyboard Layout** screen is displayed.

14. Select the appropriate language. Press **F2**. Press **Enter**.

    The system displays a popup window in the upper left corner of the screen asking if the print is legible to determine if the graphical interface of the video card is working.

15. Place the cursor in the screen and press **Enter**.

    ⚠ **CAUTION:**
    If the user does not press enter in this popup window within a short period of time, the system will exit the graphical interface installation. If this occurs, the remaining installation instructions will not align with the information displayed on the screen. Toggle the system power and repeat Booting an x86 system to the Solaris 10 DVD on page 25.

16. Select the appropriate language. Press **Enter**.

    The system displays the "**Welcome**" screen.

Note:
Do not select **Next**.

17. Continue with Configuring RAID on page 26.

Configuring RAID

This section describes how to configure RAID on SPARC and x86 systems.

1. If configuring RAID on a T4-1 platform, continue with Step 3.
2. Open a terminal window.
    a. Right click the desktop area of the screen.
    b. Select "**Programs**".
    c. Select "**Terminal...**" from the dropdown list.
3. Enter the following commands from the terminal window's command line (or the text command line on the T4-1):

```
stty erase Backspace
```

```
ksh -o vi
```

4. Umount the Solaris 10 CDROM, enter:

   ```
   umount /cdrom
   ```

   Use the following table to determine the cdrom path for your system:

   CDROM Path for platform type

Platform Type	CDROM path
T5120/5220	/dev/dsk/c0t0d0s0
x86	/dev/dsk/c1t0d0s0
T4-1	/dev/dsk/c0t6d0s0

5. Enter:

   ```
   eject -f <cdrom_path>
   ```

6. Remove the Solaris 10 DVD and put it in a safe place.
7. Insert the Avaya Call Management System software disc, for the appropriate platform, SPARC or x86, into the disc drive.
8. Enter:

   ```
   ls -l /cdrom
   ```

   - If the system does not display error messages, the `/cdrom` directory exists. Continue with Step 9.
   - If the system displays an error message, the `/cdrom` directory does not exist. Enter:

     ```
     mkdir /cdrom
     ```

9. To mount the disc in the disc drive, enter:

   ```
   mount -F hsfs <cdrom_path> /cdrom
   ```

   Verify that the **setraid** file exists in the `/cdrom` directory.

10. Enter:

    ```
    ls -l /cdrom | grep setraid
    ```

    - If the **setraid** file exists, continue with Step 11.
    - If the **setraid** file does not exist, check to be sure you inserted the correct Avaya Call Management System software disc and repeat Steps 3 through 9. If the file still does not exist, the cdrom may not be mounting properly. Escalate through normal channels.

11. Copy the **setraid** file to the `/tmp` directory, enter:

    ```
    cp -p /cdrom/setraid /tmp
    ```

12. Execute the "**setraid**" script, enter:

    `/tmp/setraid`

    The system displays messages similar to the following:

```
***** IMPORTANT!! *****

The system is booted from a Solaris 10 9/10 (Update 9) DVD

If the system is being restored be sure that the system is booted from the
same version of Solaris that was used to build the original CMS system.

Please enter y to continue or press any other key to quit:
```

13. Perform one of the following actions depending on whether this is a new install or a system restore.
    - If this is a new install, continue with Step 14.
    - If the entire system is being restored due to an unrecoverable failure, verify the Solaris 10 DVD used to boot the system matches the Solaris release, Solaris version and platform type of the original system you are restoring. A mismatch in the Solaris release, Solaris version or platform type will cause the restore process to fail. Continue with Step 14.

Note:
If the **setraid** process fails to configure the RAID hardware controller, repeat this procedure. If the process fails again, escalate through normal channels.

14. Remove the Avaya Call Management System software disc and put it in a safe place.
15. Insert the Solaris 10 DVD, for the appropriate platform, SPARC or x86, into the disc drive.
16. If the platform is a T5120/T5220 or x86, continue with Step 21.
17. If the platform is a T4-1, enter **y** to continue. Press **Enter**.

    The T4-1 system will automatically reboot.
18. The system displays the **Solaris Installation Program** screen. Select the language that is appropriate for your location. Press **F2**.
19. The system displays the **Identify This System** screen. Press **F2**.
20. If the platform is a T4-1, continue with Step 26.
21. Return to the Terminal window where the `setraid` command was executed.
22. Enter **y** to continue. Press **Enter.**

    The Solaris 10 DVD is detected and remounted.
23. Close the Terminal window.
24. Return to the Solaris **Welcome** window.
25. Click **Next** to continue.

26. Continue with Selecting your network settings on page 29.

Selecting your network settings

⚠ **Important:**
The installation for the T5120 / T5220 / x86 platforms will proceed in a graphical terminal window.
The installation for the T4-1 platform proceeds in an ASCII environment. At this point, the system disables the T4-1 mouse so all interactions are performed using the keyboard. Use the space bar to select, deselect, expand or collapse items.

The system displays the Network Connectivity options to select your network settings:

1. Select **Networked**, click <Next> or press **F2** to continue.

   The system displays **Configure Multiple Network Interfaces** options.

   Note:
   If the system is equipped with more than one network interface, the system displays the **Primary Network Interface** options.

2. Select the e1000g0 interface as the primary network interface for T5120/T5220 systems, or select the igb0 interface as the primary network interface for x86 and T4-1 systems.

3. Click <Next> or press **F2** to continue.

   The system displays the **DHCP** options.

4. Select No, and then click <Next> or press **F2** to continue.

   The system displays the **Host Name** field.

5. Enter the host name.

   ⚠ **WARNING:**
   Do not use a hyphen (-) when selecting the host name of the system. The operating system can accept a hyphen (-) in the host name but some third-party tools used with CMS do not support the hyphen (-) in the host name.

   Click <Next> or press **F2** to continue.

   The system displays the IP Address field.

6. Enter an IP address, and then press <**Next**> or press **F2** to continue.

   Note:
   Unless there is a network address for the site, enter the factory default address. The IP address 192.168.2.1 is the factory default.

   The system displays **Subnet for <interface>**.

7. Enter the appropriate answer for your network, answer yes if unsure, and then click <Next> or press **F2** to continue.

   The system displays a prompt for a netmask.

8. Enter the appropriate subnet mask. The factory default subnet mask is `255.255.255.0`.

9. Click <Next> or press **F2** to continue.

   The system displays the **IPv6** options.

10. Select **Yes**, and then press <Next> or press **F2** to continue.

    Note:
    Please wait while the network is configured.

    The system displays the **Set the Default Route** options.

11. Choose one of the following steps:

    - If the Avaya CMS system connects to the network through a router, perform the following steps:

      a. Select **Specify One**.

      b. Click <Next> or press **F2** to continue.

         The system displays a router IP address field.

      c. Enter the appropriate IP address.

    - If the Avaya CMS system is not on a subnet, select **None**.

12. Click <Next> or press **F2** to continue.

13. On T4-1 systems, a confirmation screen is presented. If the information is correct, press **F2** to continue.

14. The system displays the Kerberos options.

Configuring your Kerberos security policy

To configure your security policy:

1. Verify that **No** is selected, then click <Next> or press **F2** to continue.

   On T4-1 systems, a confirmation screen is presented, press **F2** to continue.

   The system displays the **Name Service** options.

2. Select **None** for name service, and then click <Next> or press **F2** to continue.

   On T4-1 systems, a confirmation screen is presented, press **F2** to continue.

   The system displays your **NFSv4 Domain Name** options.

3. Select "**Use the NFSv4 domain derived by the System**".

4. Click <Next>or press **F2** to continue.

   On T4-1 systems, a confirmation screen is presented, press **F2** to continue.

   The system displays the **Time Zone** options.

Selecting your regional settings

To select your regional settings:

1. On T4-1 systems, proceed to step 2.

   Select **Geographical Continent/Country/Region** and then click <Next> to continue.

   The system displays the **Continent or Country** options.

2. Select the appropriate Continent or Country, then click the arrow to the left of the Continent to expand the list.

   Note:
   On T4-1 systems, **Continent/Ocean** must be selected first, then **Country/Region**, press **F2** after selecting each category.

   The system displays the Countries available for your Continent selection.

3. Select the appropriate Country, then click the arrow to the left of the Country to expand the list.

4. Select the appropriate time zone, and then click <Next> or press **F2** to continue.

   The system displays the **Date and Time** options.

5. Enter the correct date and time, and then click <Next> or press **F2** to continue.

   On T4-1 systems, a confirmation screen is presented, press **F2** to continue.

   The system displays the **Root Password** screen.

6. Enter the password twice. If you do not know the root password assigned to the system, Avaya recommends that you leave the boxes blank to assign a blank password, and then click <Next> or press **F2** to continue.

   The system displays the **Enabling Remote Services** screen.

7. Select **Yes**, and then click <Next> or press **F2** to continue.

   Note:
   The CMS build process will run a Security script that disables unneeded services.

8. Steps 8 and 9 are valid only if you have the Solaris 10 9/10 or later DVD release. The system displays the "Oracle Solaris Auto Registration" window. Uncheck the box then click <Next> or press **F2** to continue.

9. The system displays another "**Oracle Solaris Auto Registration**" window. Leave all proxy items blank and click <Next> or press **F2** to continue.

10. If the platform is a T4-1, the system completes system identification. Press **F2** to continue. Continue with Selecting the Solaris software packages on page 32.

11. If the platform is a T5120/T5220 or x86, the system displays the **Confirm Information** screen. Verify that the settings are correct. If the settings are correct, click <Confirm> to continue.
12. The system completes system identification and displays a **Welcome** window, click <Next> or press **F2** to continue.

Selecting the Solaris software packages

The **suninstall** window might require you to select an additional option before you can continue with the Solaris installation.

> **Note:**
> Package naming may have slight differences depending on the Sun platform being loaded.

The system displays a Solaris Interactive Installation window.

- If the system is a T4-1 platform, continue with Step 1.
- If the system is a T5120/T5220 or x86 platform, continue with Step 5.

1. The system displays the **Eject a CD/DVD Automatically?** window. Select `Automatically eject CD/DVD`. Press **F2** to continue.
2. The system displays a **Reboot After Installation?** window. Select `Auto Reboot`. Press **F2** to continue. The system is initialized.

   The system displays the License window.
3. Select the **Accept** box, if present, then press **F2** to **Accept License.**
4. If the system is a T4-1 platform, continue with Step 11.
5. Select <Yes> to **Auto Reboot and Eject CD/DVD after Installation**, click <Next> to continue.
6. On x86 platforms, the system displays a **Notice** window.

   ```
   You must also manually eject the CD/DVD or select a different boot device
   after reboot to avoid repeating the installation process.
   ```

   Click <Ok>.
7. The system displays the **Specifying Media** options. Select CD/DVD, and then click <Next> to continue. The system is initialized.

   The system displays the **License** window.
8. Select the **Accept** box, if present, and then click <Next> or press **F2** to **Accept License**.
9. Select **Initial**, Click <Next>.

10. Select **Custom Install**, click <Next>.

    The system displays the **Select Geographic Regions** options.

    Note:
    Select the content, place the cursor on the ▶ symbol and Press Enter to expand the list. Select a continent then Press Enter, expand the continent list and select a country, Press Enter. Select the appropriate time zone.

11. Expand the **North America** option list.

12. Select the following options:

    English (United States) (en_US)

    English (United States UTF-8) (en_US.UTF-8)

    Note:
    These may be listed as U.S.A. (en_US.ISO8859-1) and U.S.A. (UTF-8)

13. Click <Next> or press **F2** to continue.

    The system displays the **Select System Locale** window.

14. Select English (POSIX C)(C), and then click <Next> or press **F2** to continue.

    The system displays **Additional Product** options.

15. Select None, and then click <Next> or press **F2** to continue.

16. If prompted for Filesystem Type, select UFS, and then click <Next> or press **F2** to continue.

    The system displays the **Select Software Group** window.

17. Select the appropriate option from the **Custom Packages** column.

    - On T5120/T5220 and x86 platforms, Select `End User Group` in the **Custom Packages** column. Click <Next> to customize.
    - On T4-1 platforms, Select `End User System Support` in the **Custom Packages** column. Press **F4** to customize.

    Note:
    On T4-1 systems, be sure to press **F4** to customize the installation, not **F2**.

    On some platforms, the system might not display software packages in the order shown in the following lists. If one of the packages shown below does not appear on the list, ignore it. Additionally, any version numbers may differ from what is presented. In some cases, packages may already be selected or deselected as specified below.

18. Clear the following options:

    - `A Windows SMB/CIFS fileserver for UNIX`

> **Important:**
> Verify that the Windows SMB/CIFS fileserver for UNIX package has been deselected and are not partially selected. When a module is deselected a message appears at the bottom of the screen stating that the module is deselected.

If a window pops up asking about dependency checking, click <Only once>.

- A set of Java Demo Applications
- Admin/Install Java Extension Libraries

19. Select the following option:
    - AST Graphics System Software Device Driver
20. Clear the following options:
    - Apache Standard C++ Library
21. Expand the Audio drivers and applications option and clear：
    - Audio Applications
    - Audio Sound Files
22. Clear the following options:
    - Auditservice Implementation
    - Auto Registration
    - Auto encoding finder (auto_ef)
23. Select the following option:
    - Basic Networking
24. Clear the following options:
    - Basic Registration
    - Berkley DB-Base 4.2.52
25. Select the following option:
    - CD creation utilities
26. Expand the CDE End User Software option and clear:
    - PDA Syncronization for Solaris
    - Solaris CDE Image Viewer
    - Solaris Smart Card Administration GUI
27. Clear the following options:
    - Customer registration application
28. Select the following option:

- `DVD creation utilities`

29. Clear the following options:
    - `Evolution`
    - `File system Examiner`
    - `Flex Lexer`

    ⚠ **Important:**
    Verify that the Flex Lexer is cleared and is not partially selected.

    - `Font Downloader`
30. Expand the Font Libraries and clear:
    - `Standard Type Services Framework`
    - `Standard Type Services Framework (root)`
    - `Xft(X freetype) Library`
31. Expand the Font Server Cluster option and clear:
    - `X Window System Font server`
    - `X Windows System optional fonts`
32. Expand the Freeware Compression Utilities option and clear:
    - `The Info-Zip (zip) compression utility`
33. Clear the following options:
    - `Freeware Shells`
    - `Fsexam platform dependent, /file system`
    - `Fujitsu OpenGL for Solaris Runtime Libraries (may or may not be on the list depending on the Solaris 10 release)`
    - `GLIB - Library of useful routines for C programming`
    - `GNOME Accessibility`
    - `GNOME Applications`
34. Expand the GNOME Base Libraries and clear:
    - `A Spell Checker`
    - `A Spell Checker - English`
    - `A Spell Checker - English - platform independent`
    - `A Spell Checker - platform independent`
    - `Ogg Vorbis`
35. Expand the GNOME runtime and clear:

- `GNOME CORBA ORB (BOTH)`
- `GNOME audio support Framework (All 3)`
- `GNOME freeCD database access library (ALL 3)`
- `GNOME printing technology (ALL 3)`

36. Clear the following options:
    - `GNU GhostScript Fonts (Other)`
    - `GNU GhostScript Fonts (Standard)`
    - `GTK - The GIMP Toolkit`
    - `IEEE 1394 mass storage driver`
    - `IEEE 1394 AV Driver`
    - `IEEE 1394 Video Conferencing Class Driver`
    - `International Components for Unicode User Files`
    - `Internationalized Domain Name Support Utilities`
    - `JDK 1.4 I18N run time environment`
    - `JDesktop Integration components (JDIC)`
    - `JMF MP3 Plugin`
    - `Java Advanced Imaging`
    - `Java Advanced Imaging Image I/O Tools`
    - `Java DMK 5.1 minimal subset`
    - `Java Desktop System Upgrade Package Remove`
    - `Java Run Time Integration-Plugin`
    - `Java SNMP API`
37. Expand the JavaVM option and clear:
    - `J2SDK 1.4 development tools`
    - `JDK 5.0 Dev. Tools (1.5.0_24)(the Solaris 10 Update 10 version is 1.5.0_30)`
    - `JDK 6.0 Dev. Tools (1.6.0.26)(clear only for SPARC systems, leave checked for x86 and T4-1 systems)`
    - `JavaHelp Development Utilities`
    - `SUNWj3rt post configuration`
38. Expand the Line Printer Support option and clear:
    - `ImageMagik - Image Manipulation Utilities and Libraries`
    - `a2ps - GNU Any to PostScript filter (root)`

- a2ps - GNU Any to PostScript filter (user)
- foomatic - filters - Foomatic Print Filters (root)
- foomatic - filters - Foomatic Print Filters (user)
- foomatic_ppds - Foomatic Print PPDS
- gimpprint - Drivers for Canon, Epson, Lexmark, and PCL print
- hpijs - HP InkJet Server
- psutils - PostScript Utilities

39. Clear the following options:
    - Live Upgrade Software
    - Localization common files
    - M64 Graphics Accelerator Support (may or may not be on the list depending on the Solaris 10 release)
    - MP Print Filter
    - Mozilla
    - Mozilla 3rd Party Plugins (may or may not be on the list depending on the Solaris 10 release)
40. Select the following option:
    - On-Line Manual Pages
41. Clear the following options:
    - Patch Manager Software
    - PostgresSQL
    - PostgresSQL 8.2
    - PostgresSQL 8.3
    - PostgresSQL Upgrade Tools
    - Power Management OW Utilities
    - Power Management Software
    - Print utilities for CTL Locales
42. Expand the Programming tools and libraries option and select:
    - Solaris Bundled tools
43. Expand the Remote network services and commands option and clear:
    - Trivial File Transfer Server (Root)
    - Trivial Name Server (Root)
    - Trivial Name Server (Usr)

44. Clear the following options:
    - `Resource Management WBEM Instrumentation (root)`
    - `Resource Management WBEM Instrumentation (usr)`
    - `SLP, (Root)`
    - `SLP, (Usr)`
    - `SUNWCbrowser`
45. Expand the SUNWCbrowser option (cleared above) and select:
    - `Pixman library (select only for x86 and T4-1 systems, leave cleared for T5120/T5220 systems)`
46. Select the following options:
    - `SUNWCvts`
47. Clear the following options:
    - `SW Update Manager`
    - `Service Tags`
    - `Solaris Common Agent Container`
48. Expand the Solaris Management Agent option and select:
    - `System Management Agent files and libraries`

    Deselect the following options:
    - `System Management Agent Startup scripta`
    - `System Management Agent applications and utilities`

    ⚠ **Important:**
    Verify that only Solaris Management Agent files and libraries is selected.
49. Expand the Solaris PPP option and select:
    - `Solaris PPP Device Drivers`
    - `Solaris PPP Tunneling`
    - `Solaris PPP configuration files`
    - `Solaris PPP daemon and utilities`
50. Clear the following options:
    - `Solaris Product Registry Viewer`
    - `Solaris Resource Capping Daemon`
51. Expand the Solaris Smartcard Framework option and clear:
    - `Java Communications API (may or may not be on the list depending on the Solaris 10 release)`

- `PAM Smart Card module`
- `PS/SC-Lite SCF shim`
- `SCM Smartcard Reader IFD Handler (may or may not be on the list depending on the Solaris 10 release)`
- `Sun ISCRI Kernel (May or may not be on the list depending on your platform)`
- `USB CCID IFD Handler`
- `iButton OCF CT Driver (may or may not be on the list depending on the Solaris 10 release)`

52. Clear the following options:
    - `Solaris Zones`
    - `Solstice Enterprise Agents`
    - `Spell Checking Engine - Base Release (English)`
    - `StarOffice 8.0 (may or may not be in list depending on Solaris 10 release)`
53. Select the following option:
    - `Sun Firmware Flash Update Tool (fwflash)`
54. Expand Sun Gigaswift Ethernet Adapter Software option and select:
    - `Sun Gigaswift Ethernet Adapter Driver`
55. Clear the following options:
    - `Sun IEEE1394 Framework`
    - `Sun IEEE1394 Video Conferencing Support (usr)`
    - `Sun Java(tm)Calendar preview`
    - `Sun Java(tm)Desktop System Configuration Adapter for Java Preferences`
    - `Sun Java(tm)Desktop System Configuration Agent`
    - `Sun Java(tm)Desktop System Configuration Agent Miscellaneous Files`
    - `Sun Java(tm)Desktop System Configuration Agent Wizard`
    - `Sun Java(tm)Desktop System Configuration Shared Libraries`
    - `Sun Java(tm)Desktop System launch menu integration for Configuration`
    - `Sun Update Manager Bootstrapper`
    - `Sun Update Manager Bootstrapper (root)`

- `Sun Wrapper Library for libusb; user level usb ugen library`
- `Sun (tm) Web Console`

56. Select the following option:
    - `System Accounting`
57. Clear the following option:
    - `Tcl - Tool Command Language`
58. Select the following option:
    - `Terminal Information`
59. Clear the following options:
    - `Thai partial locale pkgs`
    - `The XML lib - Python Bindings`
    - `The XSLT lib - Python bindings`
    - `Tk -TCL GUI Toolkit`
    - `Tomcat Servlet/JSP Container`
60. Clear the following options:
    - `VNC viewer client`
    - `Version info for Java Desktop System`
    - `WBEM Providers (usr)`
    - `Web Based Enterprise Management (WBEM) Services`
    - `X Windows System Minimum Required Fonts for Multibyte Locales`
61. Expand the X Windows System Runtime Environment option and Clear:
    - `X Windows System Virtual Servers`
    - `X Windows System XST extension`
    - `X Windows System demo images`
    - `X Windows System demo programs`
    - `X.Org Foundation X Client programs (clear only for T5120/T5220 systems, leave checked for x86 and T4-1 systems)`
    - `X.Org Foundation X11 cursor themes (clear only for T5120/T5220 systems, leave checked for x86 and T4-1 systems)`
62. Select the following option:
    - `X Window system online user man pages`

- `X.Org Foundation Xserver (select only for x86 and T4-1 systems, leave cleared for T5120/T5220 systems; may or may not be in the list depending on Solaris 10 release)`
- `X.Org Foundation XClient Programs (select only for x86 and T4-1 systems, leave cleared for T5120/T5220 systems; may be displayed as X.Org Foundation XClient programs documentation)`

63. Clear the following options:
    - `X11 Arabic required fonts`
    - `X11 ISO-8859-x optional fonts`
64. Expand the X11 ISO-8859-x required fonts option and Clear:
    - `Russian 1251 fonts`
    - `X11 KOI8-R fonts`
65. Clear the following options:
    - `X11/VNC Server`
    - `XSH4 conversion for Eastern European locales`
    - `XSH4 conversion for ISO Latin character sets`
    - `Xscreensaver`
    - `Xorg X libraries (clear only for SPARC systems, leave checked for x86 and T4-1 systems)`
    - `Xorg X Server (clear only for SPARC systems, leave checked for x86 and T4-1 systems)`
    - `ZFS Administration for Sun Java™ Web Console (Root)`
    - `ZFS Administration for Sun Java™ Web Console (Usr)`
66. Expand the en_us.UTF-8 option and clear:
    - `Indic (UTF-8) iconv modules for UTF-8`
    - `Japanese iconv modules for UTF-8`
    - `Korean (UTF-8) iconv modules for UTF-8`
    - `Simplified Chinese (EUC) iconv modules for UTF-8`
    - `Thai (UTF-8) iconv modules for UTF-8`
    - `Traditional Chinese (EUC) iconv modules for UTF-8`
67. Clear the following options:
    - `espgs - ESP Ghostscript (may or may not be in the list depending on Solaris 10 release)`
    - `gcmn - Common GNU package`

- `ggrep - GNU grep utilities`
- `gtar - GNU tar`
- `ipmitool (root)`
- `ipmitool (usr)`
- `jpeg - The Independent JPEG Groups JPEG software`
- `libtiff - library for reading and writing TIFF`
- `mediaLib End User Pkgs`
- `pgAdmin III`
- `pilot-link - Palm Handheld Glue`

68. Select the following options:
    - `tcpd - access control facility for internet services`
    - `utility for writing to CD-RW and DVD{+-}R/RW disks`
69. Click <Next> or press **F2** to continue.
70. Select OK or press **F2** to continue.

    The system displays a Confirmation screen.
71. Select OK or press **F2** to continue.

    The system displays a screen about package dependencies.
72. Click ignore dependencies.

    Use the following table to determine which boot disk to select:

Platform	**Boot disks**
Sun SPARC Enterprise T5120	Boot - c1t0d0
Sun SPARC Enterprise T5220	Boot - c1t0d0
Sun Netra X4270	Boot - c0t0d0
Sun SPARC T4-1	Boot - c1t0d0

- If this is a T5120/T5220 or T4-1 platform, the system displays the `Disk Selection` options. Continue with Configuring the disk drives for T5120/T5220/x86 on page 43, or Configuring the disk drives for T4-1 on page 45.

  The system displays the `Select disks for fdisk Partition Customization` options.

73. To select the disk, click in the box next to the disk name. Click <Next> to continue.

    The `Customization fdisk Partitions - Disk cxtyd0` screen is displayed.

74. Click <Next> to continue.

Configuring the disk drives for T5120/T5220/x86

To configure the disk drives:

1. Select the correct boot device, and then click <Next> to continue.

   Note:
   If the system does not display the logical device, contact your Avaya authorized service representative.

   The system displays the **Preserve Data?** options.

2. Select **no,** Click <Next> to continue.

   The system displays the **Layout File Systems?** options.

   You must load a Volume Table of Contents (VTOC) file which contains the disk partition information for the specific platform. Loading this file eliminates the need to manually calculate and enter the disk partition size and starting cylinder information which ensures the disk partitions will be correct.

3. Select **Load VTOC**.

   The system displays a popup window along with a warning message similar to the following:

```
Warning!

     Loading the existing slices for disk <boot_disk> overwrites any changes
     you made to that disk's layout.  Any slices you previously marked as
     preserved will no longer be preserved.
```

   To accept the changes, select:

4. **Load VTOC**.
5. To continue, click **Next**.

   The partition names must be manually entered into the disk layout form via the **Modify** option.

6. To display the **Modify** option, click **Back**.
7. To open the disk layout form, click **Modify**.

8. Click the cylinder tab to display the disk layout in cylinders. The cylinder tab is located at the bottom of the disk layout form.

   Click **Cyl.**

   The system displays the current partition information in cylinders.

9. Use the Slice Name information from the table below to assign names to each slice.

   Slice names for systems with 146-GBdisks

   WARNING:
   Do not click on the (MB) tab or change any values other than the Slice name. If the (MB) tab is selected, Solaris will try to automatically set up the starting cylinder values, and the Configuring the disk drives for T5120/T5220/x86 procedure will have to be repeated from the beginning.

Slice	Slice Name
0	/
1	swap
3	/cms
4	/var
5	/opt
6	/export/home
7	*(leave blank)*

   Slice names for systems with 300-GBdisks

Slice	Slice Name
0	/
1	swap
3	/cms
4	/var
5	/storage
6	/export/home
7	*(leave blank)*

   Verify the slice names entered are correct.

10. To accept the changes, click **Apply.**

11. To save the changes, click **OK**.

    The system displays the new file system layout.

12. Recheck that the correct slice name is displayed for each partition.

    - If the slice names are correct, click <**Next**> to continue.
    - If the slice names are not correct, click <**Back**> to correct the entries. Repeat the steps in procedure Configuring the disk drives for T5120/T5220/x86.

    The system displays the **Ready to Install** window.

13. Click **Install Now** to continue.

    Note:
    The x86 platform does not automatically eject the DVD even though the option was selected. Be sure to monitor the installation process which takes about 15-20 minutes and remember to eject the DVD before the system completes the reboot. It is safe to power the system off and back on in order to remove the DVD.

14. Continue with Completing the Solaris installation on page 48.

Configuring the disk drives for T4-1

To configure the disk drives:

1. Select the correct boot device, and then press **F2** to continue.

   Note:
   If the system does not display the logical device, contact your Avaya authorized service representative.

   The system displays the `Preserve Data?` options.

2. Press **F2** to continue.

   The system displays the **Automatically Layout File Systems** screen.

3. Press F4 for Manual Layout.

   The system displays the **Filesystem and Disk Layout** screen.

4. Press **F4** for Customize.

   The system displays the Customize Disk: c1t0d0 screen.

5. Press F4 for Options.

   The system displays the **Disk Editing Options** screen.

   You must load a Volume Table of Contents (VTOC) file which contains the disk partition information for the specific platform. Loading this file eliminates the need to manually calculate and enter the disk partition size and starting cylinder information which ensures the disk partitions are correct.

6. Select **Cylinders** from the “**Show size in**” options.

7. Select **Load existing slices** from VTOC label in the "**Other Options**" and press **F2** to continue.

   The system displays a warning message similar to the following:

```
Warning!

Loading the existing slices from disk will overwrite any changes you made
to that disk’s layout. Any slices marked as preserved will become
unpreserved.
```

Slice names for systems with 146-GBdisks

8. Press **F2**.

   The system displays the partitioning information for the disk. The partition names must be entered manually.

9. Use the **Slice Name** information from the table below to assign names to each slice.

Slice	Slice Name
0	/
1	swap
3	/cms
4	/var
5	/opt
6	/export/home
7	(leave blank)

Slice names for systems with 300-GBdisks

Slice	Slice Name
0	/
1	swap
3	/cms
4	/var
5	/storage
6	/export/home
7	(leave blank)

Verify the slice names entered are correct.

10. To accept the changes, press **F2**.

    The system displays the new file system layout.

11. Recheck that the system displays the correct slice name for each partition.
    - If the slice names are correct, press **F2** to continue.
    - If the slice names are not correct, press **F3** to correct the entries. Repeat the steps in procedure Configuring the disk drives for T4-1 on page 45.

    The system displays the **Mount Remote File Systems** screen.

12. Press **F2** to continue.

    The system displays the **Profile** screen.

13. Press **F2** to begin the Solaris 10 installation.

    The system displays a warning screen about configuring the default boot device.

14. Press **F2** to continue.

    ⚠ **Important:**
    The T4-1 system will automatically reboot after the Solaris 10 installation completes. The system will reboot to a command line rather than displaying the graphical **Welcome** screen. The commands in steps 15 and 16 must be executed to enable the graphics console.

15. Log in as root.

16. Enter the following commands in succession:

```
ln -s /dev/fbs/ast0 /dev/fb
```

Note:
The link may already exist, if so, ignore the "File exists" warning.

```
fbconfig -xserver Xorg
```

```
reboot
```

17. Continue with Completing the Solaris installation on page 48.

Completing the Solaris installation

⚠ **Important:**
Wait for the graphical login screen to appear. It may take several minutes to come up graphically after the installation.

To complete the Solaris installation after the system reboots, perform the following steps:

- If the system is a T5120/T5220 or T4-1 platform, the system displays the console login screen. Continue with step 1.
- If the system is a x86 platform, the system displays the OS boot option screen. Select the Solaris 10 9/10 <version> option. Continue with Configuring the Solaris operating system on page 49.

1. Enter root for the user name, followed by your password (if you submitted one to the system).

   The system displays a window giving the choice of Java Desktop System or common Desktop Environment (CDE).

2. Select Common Desktop or Common Desktop Environment (CDE).
3. Select <OK>.

   The system may display a pop-up stating CDE is deprecated, Select “Do not show this message again”.

4. Select <OK>.

Configuring the Solaris operating system

This section contains the procedures used to configure the Solaris operating system software for your Avaya CMS hardware platform.

This section includes the following topics:

Prerequisites

Before you begin any of the installation procedures:

- Verify that the Solaris 10 operating system has been installed.
- Verify that all hardware components of the system, including port cards, external disk drives, and tape drives, are correctly installed. Otherwise, the system hardware will not be recognized.
- Verify that you are logged in as **root**.

Remote terminal access tip

When executing commands that take a long time to complete, (such as `cpio` commands), use the `nohup` command to ensure that the command will complete without interruption if the data line disconnects. An example of the `nohup` command is shown below:

```
nohup cpio -icmudf -C 10240 -I <backup_media_path> "cms" | tee
```

When system reboots are required, verify that your terminal type is set correctly after the reboot.

Opening a terminal window

This section describes how to open a terminal window. You must open a terminal window to input keyboard commands at the system prompt.

To open a terminal window:

1. Use the mouse to move the cursor to an empty area of the desktop display and click the right button on the mouse.

   The system displays the `Workspace menu`.

2. Select the `Tools` option.

   The system displays the `Tools menu`.

3. Select the `Terminal` option.

   The system displays a terminal window with the active cursor at the command prompt.

Enabling the Korn shell

To enable the Korn shell:

1. Enter:

   `stty erase` **Backspace**

   The system displays the **Backspace** as `^H`. On some systems **Backspace** will not work. If this is the case, substitute `"^H"` for **Backspace**.

2. Enter:

   ```
   ksh -o vi
   ```

Displaying and setting the EEPROM parameters (T5120/T5220/T4-1 systems only)

The current EEPROM settings must be displayed to determine if a firmware value must be changed from a factory setting.

This section includes the following topics:

- Displaying the EEPROM values on page 51
- Required EEPROM settings on page 51
- Changing EEPROM settings on page 52

Displaying the EEPROM values

To display the firmware EEPROM values for an Avaya CMS system:

1. Enter:

   ```
   eeprom | sort | more
   ```

   The system displays the current EEPROM settings.

   Note:
   Not all options are displayed for all Avaya CMS systems. In addition, some options will show `"data not available"` messages. Ignore those options.

2. Compare the displayed settings with the Required EEPROM settings on page 51 to determine if any of the values must be changed from the factory setting.

Required EEPROM settings

The following table contains the Avaya CMS EEPROM settings that might need to be reset manually. Additional EEPROM settings are set automatically during the installation. For a complete list of required EEPROM settings, see Avaya CMS EEPROM settings on page 262.

Option Name	Required setting
ansi-terminal?	`true`
boot-command	`boot`
local-mac-address?	`true`

Changing EEPROM settings

To change an EEPROM setting, enter:

eeprom *option_name=option_value*

where ***option_name*** is the name of the option, and ***option_value*** is the new setting.

Example:

To change the output device, you would enter:

eeprom auto-boot?=true

Turning on the system activity recorder

To turn on the system activity recorder:

1. Log in with the `sys` login id by entering:

   su - sys

   Note:
   Ensure you use a space between "`-`" and "`sys`".

   The prompt changes to a dollar sign (`$`).

2. Confirm that you are using the sys id by entering:

   id

   The system displays the following message:

```
uid=3(sys) gid=3(sys)
```

3. Enter the following commands to create and edit the **cron.sys** file:

   ```
   cd /tmp
   ```

   ```
   crontab -l > cron.sys
   ```

   ```
   vi cron.sys
   ```

   The **cron.sys** file looks similar to the following example:

```
#ident  "@(#)sys 1.5     92/07/14 SMI"   /* SVr4.0 1.2   */
#
# The sys crontab should be used to do performance collection.
# See cron and performance manual pages for details on startup.
#
# 0 * * * 0-6 /usr/lib/sa/sa1
# 20,40 8-17 * * 1-5 /usr/lib/sa/sa1
# 5 18 * * 1-5 /usr/lib/sa/sa2 -s 8:00 -e 18:01 -i 1200 -A
```

4. Remove the leading pound (#) characters that were used to comment out the last three lines in the file.

   Example:

```
#ident  "@(#)sys 1.5     92/07/14 SMI"   /* SVr4.0 1.2   */
#
# The sys crontab should be used to do performance collection.
# See cron and performance manual pages for details on startup.
#
0 * * * 0-6 /usr/lib/sa/sa1
20,40 8-17 * * 1-5 /usr/lib/sa/sa1
5 18 * * 1-5 /usr/lib/sa/sa2 -s 8:00 -e 18:01 -i 1200 -A
```

5. Press **Esc**. Then enter:

   ```
   :wq!
   ```

   The system saves and closes the file.

6. Enter the following commands:

   ```
   crontab -r
   ```

   ```
   crontab cron.sys
   ```

7. Enter the following command to confirm that the changes you made are intact:

   ```
   crontab -l
   ```

   The system displays the **cron.sys** file.

8. Exit superuser mode by entering:

   ```
   exit
   ```

   The prompt changes back to a pound (#) prompt.

Note:
You may have to repeat the exit step twice.

9. Run the command:

   `svcadm enable sar`

Adding the CMS fully qualified domain name to /etc/hosts

1. To edit the `/etc/hosts` file, enter:

   `vi /etc/hosts`

   The items in this file must be separated by tabs, not spaces, and any comments must begin with a #. The entry for `localhost` must remain on line four and the entry for `loghost` must remain on line five.

   The `loghost` line should contain the fully qualified domain name of the Avaya CMS system.

   The fully qualified domain name is either the customer domain name or the default entry `tempdomain.net.`

   Example:

```
#
# Internet host table
#
127.0.0.1 localhost
192.168.2.1 cms cms.tempdomain.net loghost
```

Installing the Solaris patches

Sun periodically provides updates for the Solaris operating system. The Solaris patches are delivered with the Avaya CMS software.

To install the Solaris patches:

1. Verify that you are logged into the system as **root**.
2. Load the Avaya Call Management System software disc into the disc drive.
3. Enter:

   `cd /`

4. Enter:

   `/cdrom/cdrom0/spatches_conf`

   The system displays one of the following messages:

   - If the system firmware needs to be updated, the system displays the following message:

```
WARNING: System FW must be updated to accept latest Solaris patches.
   The FW update can be installed now if you wish.
Respond to the below request with y if you wish to install FW now.
 This procedure will shutdown the system to apply the FW in ILOM and
could take 20 minutes to complete. After 20-30 minutes press the
Power button to restart the system. Will take ~15 mins. to come up
 WARNING!! Manually bypassing this check and installing the Spatches could
 leave your system unusable.
WARNING: Host will be powered down for automatic firmware update when download
is completed.
Do you want to continue(yes/no)?
```

   - If there are *no* system firmware updates or Solaris patches to install, the system displays the following message:

```
There are no Solaris patches to install
```

   Continue with Installing the Storage Manager package (T5120/T5220 systems only) on page 59.

   - If there are no system firmware updates but there are Solaris patches to install, the system displays the following message:

```
Warning: you must close all applications before running this script
...................
...................
...................
Solaris patches have been spooled to your machine.  The patches will
beinstalled after rebooting.  During the installation of patches your
server will not be available.

The estimated time to install all patches is: 15 minutes

Ready to install Patches. Please leave the CD in the drive.
You will need to reboot the server for patches to install.

Do you want to reboot now?  [y,n,?]
```

Note:

The system displays the approximate amount of time needed to install the Solaris patches.

⚠ **Important:**
You need to monitor the system during the Solaris patch installation process to ensure that the installation of the Solaris patches does not halt. Some Solaris patch updates cause the system to automatically reboot during the Solaris patch installation process. The Solaris patch installation process takes at least the amount of time that was estimated earlier in the procedure. It is possible that the system will power off as part of a Solaris patch installation. If the system powers off, you need to manually power on the system by pressing the power button. In some cases the system can power off before a Solaris patch is actually installed which means that the patch can install during boot up after you press the power button. The system can automatically power off again after the patch installs. If this occurs, you need to manually power on the system again. When the Solaris patch installation process completes, the system will automatically reboot into multiuser mode and the system displays the graphical login screen.

5. If the system firmware needs to be updated, continue with Step 7.
6. If there are no system firmware updates but there are Solaris patches to install, continue with Step 11.
7. Update the system firmware. Enter **yes**.

⚠ **Important:**
If you answer **yes** to updating the system firmware, only the system firmware is updated. Once the system firmware is updated, the user must re-run the `spatches_conf` script to determine if any additional Solaris patches must be installed.

⚠ **CAUTION:**
Manually bypassing firmware updates and installing spatches can leave your system unusable. The system is powered down as part of the firmware update. Some Solaris platforms automatically power back on after the firmware updates are applied while other platfomrs do not. Allow 20-30 minutes for the firmware to be updated. If the system does not automatically power on, press the Power button to restart the system.

8. Monitor the system as the firmware is updated. If the system does not power on after 30 minutes, press the power button.
9. After the graphical console returns, log in to the system as `root`.

10. Enter:

    `/cdrom/cdrom0/spatches_conf`

    If there are Solaris patches to install, the system displays the following message:

```
Warning: you must close all applications before running this script
...................
...................
...................
Solaris patches have been spooled to your machine.  The patches will
be installed after rebooting.  During the installation of patches
your server will not be available.

The estimated time to install all patches is: 15 minutes

Ready to install Patches. Please leave the CD in the drive.
You will need to reboot the server for patches to install.

Do you want to reboot now?  [y,n,?]
```

11. Install the Solaris patches by entering **`y`**.

    ⚠ **CAUTION:**
    If you cancel the installation of Solaris patches, you must install them before upgrading CMS. To cancel installation of the Solaris patches, enter **`n`**.

    The system boots into single user mode and begins to install the Solaris patches. The Solaris patch installation takes at least the amount of time that was estimated earlier in the procedure. After the Solaris patches are installed, the system reboots into multiuser mode and displays a login prompt.

    ⚠ **CAUTION:**
    Solaris 10 does not display the Solaris patches on the console as they install. The display can become blank for at least the time the Spatches installer reports at the end of Step 10. Once the graphical console returns, the system has completed the Solaris patches installation. Do not halt the system.

12. Monitor the Solaris patch installation process to ensure that the system has not powered off as a result of the installation of a particular Solaris patch. If the system has powered off, press the power button to power the system back on. Refer to the Important message in step 5 for more information.

13. Log into the system as **root**.

14. If `auto-boot?` was set to false in Step 6 then enter:

    `eeprom auto-boot?=true`

15. Verify that all of the Solaris patches have been installed by entering:

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

    The system displays the following message in the log:

```
All patches installed successfully.
```

Note:

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

```
Installation failed for one or more Solaris patches.

- 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.
Patch installation completed: Fri Jan 18 13:28:19 MST 2002
```

If the message shown above is displayed, continue with this procedure and the remaining Avaya CMS base load upgrade procedures. When the upgrade is complete, notify your Avaya CMS support organization as instructed.

For additional information on Solaris patches, see Working with Solaris patches on page 193.

Installing the Storage Manager package (T5120/T5220 systems only)

1. Insert the Avaya Call Management System software disc, for the SPARC platform, into the disc drive.
2. Install the StorMan package, enter:

   ```
   /usr/sbin/pkgadd -d /cdrom/cdrom0/StorMan.pkg
   ```
3. Enter: **`all`**
4. Answer **`y`** to any prompts.
5. Repeat the steps in the section Installing the Solaris patches on page 54.

Note:

Repeating the Solaris patch installation procedure is necessary after the original Spatches install because a critical patch may be needed to allow the system to automatically mount the Solaris Sun StorageTek™ RAID SPARC Configuration disc. If the patch is not included, the system volfs service will fail and drop a core file in the system / directory.

Installing the MegaRAID Utility packages

Note:

Only load this package set if you have r16.2da.k or later. If you have an earlier release, the package will not be on your Avaya Call Management System software disc.

1. Insert the Avaya Call Management System software disc, for the appropriate platform, SPARC or x86, into the disc drive.
2. Install the Solaris gccruntime package, enter:

   ```
   /usr/sbin/pkgadd -d /cdrom/cdrom0 SUNWgccruntime
   ```
3. Answer **`y`** to any prompts.

   Note:

   This package installation may return an error that the package is already installed. If so, continue with installing the MegaCli package.
4. Install the MegaCli package, enter:

   ```
   /usr/sbin/pkgadd -d /cdrom/cdrom0/MegaCli.pkg
   ```
5. Enter: **`all`**

6. Answer **`y`** to any prompts.

Installing the Avaya CMS security script

To install the Avaya security script:

Important:
You will be able to log into the console only as **root** after you run the Avaya CMS security script. If you are logging into the system remotely, you will need to log in as another user and then su to root.

1. Verify that you are logged into the system as **root**.
2. Load the Avaya Call Management System software disc into the disc drive.
3. Enter:

   `cd /`
4. Enter:

   `/cdrom/cdrom0/security/cms_sec`

   The system configures your security settings. This process will take some time. The system 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.

5. Reboot the system by entering:

   `/usr/sbin/shutdown -i6 -g0 -y`

   Log into the system as **root**.

Installing Avaya CMS and supporting software

This section contains the procedures used to install and set up the Avaya Call Management System (CMS) software and other supporting software.

This section includes the following topics:

Installation rules

If the software was installed at the factory, the only procedures required at the customer site are:

- Configuring Avaya CMS authorizations on page 67
- Installing feature packages on page 102

If the Avaya CMS software was not installed at the factory, use the procedures in Installing the Solaris operating system on page 19, Configuring the Solaris operating system on page 49, and this chapter to bring the Avaya CMS system up to factory standards after a system re-configuration or repair.

Installing Informix

Informix provides the relational database management system used to organize Avaya CMS data. Avaya CMS works in conjunction with the Informix software.

This section includes the following topics:

- Prerequisites on page 62
- Installing Informix on page 62
- Initializing the Informix database on page 63

Prerequisites

Before you begin installing the Informix software packages, perform the following tasks:

- Verify that you are logged in as **root** at the console.
- Obtain the Avaya CMS R16.3 Software Installation disc.

Installing Informix

To install the Informix software:

1. Open a terminal window.
2. To enable Korn shell, enter:

   ```
   ksh -o vi
   ```

3. Insert the Avaya Call Management System software disc, for the specific platform type such as SPARC or x86, into the disc drive.
4. Start the installation of the Informix SQL packages by entering:

   ```
   /cdrom/cdrom0/install_informix.sh
   ```

   The system completes the installation of the Informix packages.

Initializing the Informix database

To initialize Informix Dynamic Server (IDS) for Avaya CMS:

1. Set the Informix environment by entering:

   `. /opt/informix/bin/setenv`

2. Initialize the database by entering:

   `/opt/informix/bin/dbinit.sh`

3. Verify the IDS is On-Line by entering:

   `onstat -d | grep On-Line`

   The system displays an On-Line message and several sets of data..

```
Informix Dynamic Server Version XX.XX.FCX -- On-Line -- Up 00:00:55 --
xxxxxx Kbytes
```

Installing the Avaya CMS Supplemental Services software

To install the Supplemental Services software:

1. Verify that you are logged in as **root** at the console.
2. Record the Avaya CMS Supplemental Services version number printed on the Avaya CMS R16.3 Software Installation disc. You will need this number during the procedure.

Version number	

3. Insert the AVAYA CMS Supplemental Services for CMS R16.3 software disc into the disc drive.
4. Enter:

   `/usr/sbin/pkgadd -d /cdrom/cdrom0 LUim`

   The system loads the Installation Manager, Explorer and Memory tools software. The system displays the following message when the installation is complete:

```
Installation of <LUim> was successful.
```

5. Enter:

   `/opt/LUim/bin/install 2>&1 | tee -a /opt/LUim.log`

   The system displays the following message:

```
Using </opt/SUNWexplo> as the package base directory.
..............
..............
..............
Do you want to install these conflicting files [y,n,?,q]
```

6. Enter: **`y`**

```
This package contains scripts which will be executed with super-user permission
during the process of installing this package.
..............
..............
..............
Do you want to continue with the installation of <SUNWexplo> [y, n,?]
```

7. Enter: **`y`**

   The system displays the following message:

```
Installing Sun(TM) Explorer Data Collector as <SUNWexplo>
.............
.............
.............
====== Installation of Supplemental Services Completed === current date and
time
```

8. Perform one of the following actions (for T5120/T5220/T4-1 systems only):

   - If the system does not display a license agreement for the SUNWexplo package, or if the system displays a message "`CTEact already installed`", go to Step 9.
   - If the system does display a series of questions about the SUNWexplo package, accept the default answers when provided.

9. Enter:

   `/opt/cc/install/ahl.cssr16`*`YXX.X`*`/bin/setup`

   where ***Y*** is the platform type (S for T5120/T5220/T4-1, X for x86) and ***`XX.X`*** is the Avaya CMS Supplemental Services version number you recorded earlier in Step 2 of Installing the Avaya CMS Supplemental Services software on page 63.

   The system displays the following message:

```
No previous version is in place.
enable crontab entry...
set up output log configuration...
AHL setup completed successfully.
```

10. Enter:

    ```
    /opt/cc/install/aot.cssr16YXX.X/bin/setup
    ```

    where *Y* is the platform type (S for T5120/T5220/T4-1, X for x86) and ***XX.X*** is the Avaya CMS Supplemental Services version number you recorded earlier in Step 2 of Installing the Avaya CMS Supplemental Services software on page 63.

    The system displays the following message:

```
No previous version is in place.
.
.
.
AOM setup completed successfully.
```

Installing the Avaya CMS packages

This section contains procedures for the installation and configuration of the Avaya CMS software.

This section includes the following topics:

- Prerequisites on page 65
- Installing the Avaya CMS software on page 66
- Configuring Avaya CMS authorizations on page 67
- Installing the Avaya CMS patches on page 73
- Storage requirement for CMS on page 75

Prerequisites

Before you install any of the Avaya CMS packages, perform the following tasks:

- Verify that you are logged in as **root** at the console.
- Obtain the Avaya CMS R16.3 Software Installation disc.
- Obtain the current CMSSVC password.

> ⚠ **Important:**
> The CMSSVC login is used only by Avaya services personnel. Do not give out the CMSSVC password.

Installing the Avaya CMS software

To install the Avaya CMS software:

1. Load the Avaya CMS R16.3 Software Installation software disc into the disc drive.
2. Enter:

   `cd /`

3. Add the Avaya CMS package by entering:

   `/usr/sbin/pkgadd -d /cdrom/cdrom0 cms`

   Important:
   During the installation, the system might display conflicting file messages. Enter **`y`** to install any conflicting files.

   The system begins the installation and then displays the following message:

```
Assigning a new password for cms
New password:
```

4. Enter the password for the Avaya CMS login.

   The system displays the following message:

```
Re-enter new password:
```

5. Re-enter the password for the Avaya CMS login.

   The system displays the following message:

```
passwd (SYSTEM): passwd successfully changed for cms

Creating cmssvc user id
6 blocks
Assigning a new password for cmssvc
New password:
```

6. Enter the password for the CMSSVC login.

   The system displays the following message:

```
Re-enter new password:
```

7. Re-enter the password for CMSSVC.

   The system begins to install the Avaya CMS software.

8. Press the **Enter** key to continue the display.

Note:
It might be necessary to enter **y** several times to install any conflicting files.

The system finishes installing the Avaya CMS software, and displays the following message:

```
If CMS was installed by choosing cms from the pkgadd menu, type q and press
return to exit.

If cms was installed using pkgadd -d /cdrom/cdrom0 cms, press return.

Installation of <cms> was successful.
```

9. Press **Enter**.
10. Perform one of the following tasks:
    - If the system prompts you to reboot the system, perform the following steps:
        a. Enter:

           `/usr/sbin/shutdown -y -i6 -g0`

           The system reboots.

        b. Log in as **root**.
    - If the system does not prompt you to reboot the system, go to Configuring Avaya CMS authorizations on page 67.

Note:
If you have problems installing the Avaya CMS software, see Avaya CMS installation fails on page 260.

Configuring Avaya CMS authorizations

This section describes how TSC personnel set authorizations for Avaya CMS features that are purchased by the customer. Authorizations apply to all ACDs that are administered. You can use the `auth_set` option in the `Avaya Call Management System Services Menu` to:

- Set the purchased version of Avaya CMS
- Authorize packages and features
- Change the number of agents, ACDs, or Supervisor logins

To set authorizations for Avaya CMS features:

1. TSC personnel should verify that the on-site technicians have completed the following tasks:
    - Connected the console to the Avaya CMS system

- Connected the Avaya CMS system to the TSC’s Remote Maintenance Center (remote console)
- Connected the link between the Avaya CMS system and the switch

Note:
If the hardware link or the Automatic Call Distribution (ACD) feature and Avaya CMS is not properly administered, the Avaya CMS software cannot communicate with the switch. For switch administration procedures, see *Avaya Call Management System Switch Connections, Administration, and Troubleshooting*.

2. Enter:

   `cmssvc`

   The system displays a warning that IDS is off, then displays the **Avaya 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) patch_inst     Install a single CMS patch from CD
9) patch_rmv      Backout an installed CMS patch
10) load_all      Install all CMS patches found on CD
11) back_all      Backout all installed CMS patches from machine
Enter choice (1-11) or q to quit:
```

3. Enter the number associated with the **run_ids** option.

   IDS is turned on.

4. Enter:

   `cmssvc`

   The system then displays the **Avaya Call Management System Services** menu .

5. Enter the number associated with the **auth_set** option.

   The system displays the following message:

```
Password:
```

6. Enter the appropriate password.

Important:
The **auth_set** password is available only to authorized Avaya personnel.

Note:
Some of the following questions may not be displayed if the authorization cannot be changed at this time.

The system displays the following message:

```
Is this an upgrade? (y/n):
```

Note:
This question occurs the first time you run **auth_set** on the system.

7. Perform one of the following actions:

   - If this is not an upgrade,

     a. Enter: **`n`**

        The system displays the following message:

```
Purchased version is R16.3. Is this correct? (y/n):
```

     b. Enter: **`y`**

   - If this is an upgrade, enter: **`y`**

   The system displays the following message:

```
Authorize installation of forecasting package? (y/n):(default: n)
```

8. Perform one of the following actions:

   - If the customer purchased the forecasting package, enter: **`y`**
   - If the customer did not purchase the forecasting package, enter: **`n`**

   The system displays the following message:

```
Authorize use of graphics feature? (y/n): (default: n)
```

9. Perform one of the following actions:

   - If the customer purchased the graphics feature, enter: **`y`**
   - If the customer did not purchase the graphics feature, enter: **`n`**

   The system displays the following message:

```
Authorize use of external call history feature? (y/n): (default: n)
```

10. Perform one of the following actions:

    - If the customer purchased the external call history feature, enter: **`y`**

- If the customer did not purchase the external call history feature, enter: **n**

The program responds (if the vectoring package is authorized):

```
Authorize use of expert agent selection feature? (y/n): (default: n)
```

11. Perform one of the following actions:
    - If the customer purchased the expert agent selection feature, enter: **y**
    - If the customer did not purchase the expert agent selection feature, enter: **n**

    The system displays the following message:

```
Authorize use of external application feature? (y/n):(default: n)
```

12. Perform one of the following actions:
    - If the customer purchased the external application feature, enter: **y**
    - If the customer did not purchase the external application feature, enter: **n**

    The system displays the following message:

```
Authorize use of global dictionary/ACD groups feature? (y/n):
(default: n)
```

13. Perform one of the following actions:
    - If the customer purchased the global dictionary/ACD groups feature, enter: **y**
    - If the customer did not purchase the global dictionary/ACD groups feature, enter: **n**

    The system displays the following message:

```
Enter the number of simultaneous Avaya CMS Supervisor logins the
customer has purchased (2-maximum): (default: 2)
```

14. Enter the number of simultaneous logins purchased by the customer.

    The system displays the following message:

```
Has the customer purchased Avaya Report Designer? (y/n): (default:
n)
```

15. Enter: **y**

    The system displays the following message:

    ```
    Enter the maximum number of split/skill members that can be
    administered (1-maximum):
    ```

    “Split or skill members” are defined as the number of CMS-measured agent-split and agent-skill combinations that are logged in at the same time. Each split that an agent logs into is an agent-split combination. Each skill that is assigned to an agent while the agent is logged in is an agent-skill combination.

    The minimum size configuration for Avaya CMS is 20. The maximum number of split skill members across all ACDs is documented in the *Avaya Aura™ Communication Manager System Capacities Table*. Your platform configuration and switch interval could change the number of split skill members you can have on your system.

    You can limit the split or skill random access memory (RAM) allocation to the size that is actually needed for the current configuration of agents and splits or skills. This is accomplished by the total split/skill members summed over all splits/skills fields, which is accessed through the `setup` option of the **`cmssvc`** command.

    The recommended numbers for Expert Agent Selection (EAS) and non-EAS systems are shown in the following table.

CMS agent Right to Use (RTU)	Total logged-in agents across all ACDs	Split/skill members provisioning	
		Non-EAS (Maximum of 4 splits per agent)	EAS (Maximum of 100 skills per agent)
20	20	100	1200
100	100	400	6000
200	200	1000	12,000
300	300	1200	18,000
400	400	1600	24,000
500	500	2000	30,000
600	600	2400	36,000
700	700	2800	42,000
800	800	3200	48,000
900	900	3600	54,000

CMS agent Right to Use (RTU)	Total logged-in agents across all ACDs	Split/skill members provisioning	
		Non-EAS (Maximum of 4 splits per agent)	EAS (Maximum of 100 skills per agent)
1000	1000	4000	60,000[1]
1500	1500	6000	90,000
2000	2000	8000	150,000[2]
3000	3000	12,000	150,000
4000	4000	16,000	150,000
7000	7000 or greater	20,800 up to 150,000	150,000

[1] Going above 1000 logged-in agents in the single switch environment requires that the average skills per agent be less than 100 since 150,000 skill pairs is the limit of the largest switch configuration (S8700 Media Server).

[2] The ACD switch maximum is 7000 logged in agents and 150,000 skill pairs.

16. Enter the maximum possible number of split or skill members that the customer might use based on the size of the switch agent purchased.

    The system displays the following message:

```
Enter the maximum number of ACDs that can be installed (1-8):
(default: 1)
```

17. Enter the number of ACDs the customer purchased.

    The system displays the following message:

```
Enter the number of authorized agents(Right To Use):
```

Note:
RTU is the number of agents paid for on the CMS system. This number is on the CMS order paperwork.

18. Enter the number of authorized agents.

    The system displays the following message:

```
Enter the number of authorized ODBC connection (0-10): (default: 0)
```

19. Perform one of the following actions:

- If the customer purchased ODBC connections, enter the number of ODBC connections authorized.
- If the customer did not purchase any ODBC connections, press **Enter**, the default is zero ODBC connections.

  The system displays the command prompt after all authorizations have been set.

20. Verify authorizations are correctly set by entering:

    ```
    cmssvc
    ```

    The system then displays the **Avaya Call Management System Services** menu.

21. Enter the number associated with the `auth_display` option.

22. Verify that the administration completed successfully by entering:

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

    The system displays the **admin.log** file. The **admin.log** file contains information related to Avaya CMS administration procedures.

```
CMS Version XXXX.XX installation successful <date/time>
Authorization command started <date/time>
Capabilities/capacities authorized <date/time>
```

Note:
You can also verify the authorizations by using the **auth_display** option of the `cmssvc` command.

Installing the Avaya CMS patches

To install Avaya CMS patches:

Important:
The features must be authorized on your system before patches can be installed. To have authorizations installed, call the Avaya helpline. We recommend that you always install all available patches. For more information about patch requirements, see Avaya CMS patch requirements on page 198.

If you believe that you should not be installing a particular patch, call the National Customer Care Center at 1-800-242-2121, or consult with your product distributor or representative, before you decide not to install it.

1. Verify that the Avaya CMS R16.3 Software Installation software disc is in the disc drive.

2. Enter:

   cmssvc

   The system displays the **Avaya Call Management System Services** menu.

3. Choose one of the following actions:

   - To load all the patches, enter the number associated with the `load_all` option.
   - To load one patch at a time, enter the number associated with the `patch_inst` option.

   The system checks for patches on the software disc.

   – If no patches are found on the software disc the system displays the following message:

```
No CMS patches found on the CD.
Please check the CD and try again.
```

   – If patches are available for installation, the system responds with the following message:

```
The following patches are available for installation:
.........
.........
.........
Are you sure you want to install all these patches? (y|n)
```

4. Choose one of the following actions:

   - If no patches are found on the software disc continue with Step 5.

- If patches are found on the software disc, enter `y` to install all of the patches, or enter the patch number if you are installing only one patch.

  The system installs the patch or patches. As it does so, it displays messages similar to the following for each patch that is installed:

```
@(#) installpatch 1.0 96/04/01
cmspx-s
Generating list of files to be patched...
Creating patch archive area...
Saving a copy of existing files to be patched...
xxxx blocks
        File compression used
Installing patch packages...

Doing pkgadd of cmspx-s package:
Installation of <cmspx-s> was successful.

Patch packages installed:
        cmspx-s

Patch installation completed.
```

5. Enter:

   eject cdrom

Storage requirement for CMS

Determine how much dataspace is required for the CMS full maintenance backup.

1. Set the informix environment. Enter:

   . /opt/informix/bin/setenv

2. Enter:

   onstat -d

   The system displays the current usage information for the Informix database. Use the output generated from running this command and the formulas at the bottom of the tables to calculate how much database space is required for a CMS full maintenance backup. The data in this table is dynamic and changes as database space is used.

Current usage information for the Informix database

Platform/ cmsdbs Dbspace	nchunks	Full disk size of cmsdbs Dbspace	Total Disk cmsdbs Dbspace (Bytes)	Total Disk cmsdbs Dbspace (rounded in GB)	Total Full Maintenance Backup space Required if cmsdbs Dbspace is full (GB)[1]
146 GB Disks					
T5220	8192	40072200	3.28271E+11	305.73	10.19
T5120-4 core	8192	22164745	1.81574E+11	169.10	5.64
300 GB Disks					
T5220	8192	69585913	5.70048E+11	530.90	17.70
T5120-8 core	8192	69585913	5.70048E+11	530.90	17.70
T4-1	8192	69585913	5.70048E+11	530.90	17.70
T5120-4 core	8192	33269676	2.72545E+11	253.83	8.46
600 GB Disks					
X4270	8192	33249595	2.72381E+11	253.67	8.46

[1] If ontape is being used for binary backups this value must be multiplied by 30 since ontape does not compress data.

Bytes to GB conversion factor = 1073741824

Full Maintenance Backup compression ratio (approx.) = 30

X4270 (600 GB) example:

Dbspaces address	numbers	flags	fchunk	nchunks	pgsize	flags	owner	name	owner	name
14fb304f0	6	0x40001	6	8192	N	B	informix	cmsdbs	informix	cmsdbs

Chunks address	chunk	dbs	offset	size	free	bpages	flags	pathname	flags	pathname
14fb31028	6	6	3192656	33249595	16089149		PO-B-	/dev/rdsk/cmsdisk	PO-B-	/dev/rdsk/cmsdisk

Full Dbspace size of cmsdbs = ((8192 * 33249595) / 1073741824) = 253.67 GB

Full Dbspace size of cmsdbs available for Full maintenance backups =

(((8192 * 33249595) / 1073741824) / 30) = 8.46 GB

Space required for backup = (((8192 * (33249595 - 16089149)) / 1073741824) / 30) = 4.36 GB

Configuring the ODBC and JDBC server software

Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) allows you to access data in the Avaya CMS database for use in other software applications such as spreadsheet programs. With ODBC and JDBC, you can access the Avaya CMS data directly from your application without needing to understand database connectivity or format. ODBC and JDBC allows access to data at multiple sites for reports. The following procedures allow you to install or upgrade your ODBC and JDBC software. For more information about the ODBC and JDBC client software, see *Avaya Call Management System ODBC and JDBC*.

Setting up Avaya CMS data storage parameters

This section describes how TSC personnel modify specific data storage parameters on the Avaya CMS system. These storage parameters affect the operation of the Avaya CMS software.

⚠ **Important:**
Throughout the setup, you are prompted to enter values that are specific to the system being installed. These values differ between switch releases. For each question, an appropriate range of values is displayed. These values represent the limits of each range.

To modify Avaya CMS data storage parameters:

1. Change to the Avaya CMS installation directory by entering:

   ```
   cd /cms/install/cms_install
   ```

2. Enter:

   ```
   vi storage.def
   ```

Note:
The **storage.def** file contains the data storage parameters. The Avaya CMS system is installed with a set of standard default values. If you delete or damage the **storage.def** file, you can find a copy of this file (**storage.skl**) in the same directory.

The default storage parameters are listed in the Default Avaya CMS data storage parameters table on page 78 in the order in which they appear in the **storage.def** file. The data storage parameters are documented in the *Avaya Aura™ Communication Manager System Capacities Table.*

Default Avaya CMS data storage parameters table

Parameter	Default
Intrahour interval (15, 30, 60 minutes):	30
Week start day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday):	Sunday
Week end day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday):	Saturday
Daily start time (regular time):	12:00 AM
Daily stop time (data will be collected for seconds of last minute):	11:59 PM
Number of agent login/logout records:	10000

Default Avaya CMS data storage parameters table

Parameter	Default
Number of agent trace records:	10000
Number of call records:	0
Number of exceptions records:	250
# Days of intrahour for splits (1-62):	31
# Days of daily splits (1-1825):	387
# Weeks of weekly splits (1-520):	53
# Months of monthly splits (1-120):	13
# Days of intrahour for agents (1-62):	31
# Days of daily agents (1-1825):	387
# Weeks of weekly agents (1-520):	53
# Months of monthly agents (1-120):	13
# Days of intrahour for trunk groups (1-62):	31
# Days of daily trunk groups (1-1825):	387
# Weeks of weekly trunk groups (1-520):	53
# Months of monthly trunk groups (1-120):	13
# Days of intrahour for trunks (1-62):	31
# Days of daily trunks (1-1825):	387
# Weeks of weekly trunks (1-520):	53
# Months of monthly trunks (1-120):	13
# Days of intrahour for call work codes (1-62):	0
# Days of daily call work codes (1-1825):	0
# Weeks of weekly call work codes (1-520):	0
# Months of monthly call work codes (1-120):	0
# Days of intrahour for vectors (1-62):	31
# Days of daily vectors (1-1825):	387
# Weeks of weekly vectors (1-520):	53

Default Avaya CMS data storage parameters table

Parameter	Default
# Months of monthly vectors (1-120):	13
# Days of intrahour for VDNs (1-62):	31
# Days of daily VDNs (1-1825):	387
# Weeks of weekly VDNs (1-520):	53
# Months of monthly VDNs (1-120):	13

3. Review the default data storage values for each authorized ACD. The default values are found on the line immediately below each storage parameter.
4. Enter the values determined by the account executive, system consultant, and design center. These values are based on the customer configuration.
5. Press **Esc**. Then enter:

   ```
   :wq!
   ```

   The system saves and closes the file.

Note:
After the Avaya CMS software is running, the system administrator can change the data storage parameters using the `Data Storage Allocation` window and the `Storage Intervals` window. Both windows are accessed from the `CMS System Setup` menu.

For more information about changing Avaya CMS data storage parameters, see *Avaya Call Management System Administration*.

Setting up LAN connections

This section describes how to set up a network connection to a LAN-enabled switch and other Avaya CMS system peripherals. For more information about LAN switch configurations, see *Avaya Call Management System Switch Connections, Administration, and Troubleshooting*.

This section includes the following topics:

- Prerequisites on page 81
- Editing the /etc/hosts file on page 81
- Setting up a second network interface on page 82
- Editing the /etc/defaultrouter file on page 85

Prerequisites

Before you begin setting up the network for LAN connections, perform the following tasks:

- Verify that you are logged in as **root**.
- Verify that the Avaya CMS software is turned off and the IDS software is on.
- Verify that all file systems are mounted.
- Verify that Avaya Communication Manager 2.0 or later are installed.

Editing the /etc/hosts file

To edit the **/etc/hosts** file:

1. Enter:

   `vi /etc/hosts`

   Important:
   The items in this file must be separated by tabs, not spaces, and any comments must begin with a `#`. The entry for `localhost` must remain on line four and the entry for `loghost` must remain on line five.

   The `loghost` line should contain the Avaya CMS system:

   – IP address

   – Host name

   – Hostname.fully qualified domain name

   – `loghost`

   The fully qualified domain name is either the customer domain name or the default entry `tempdomain.net`

   Example:

```
#
# Internet host table
#
127.0.0.1       localhost
192.168.2.1   cms   cms.tempdomain.net  loghost
```

2. Add a new line to this file for each ethernet card that is installed in this computer using TCP/IP. You must enter the IP address and the host name.

   This example shows the recommended default IP addressing scheme for a closed network.

```
#
# Internet host table
#
127.0.0.1      localhost
192.168.2.1    cms   cms.tempdomain.net  loghost
216.25.242.138    cms_1    #2nd network card on seperate subnet
192.168.2.2    switch
192.168.2.103  router
```

Note:
Only the primary network card needs the fully qualified domain name.

3. Press **Esc**. Then enter:

   `:wq!`

   The system saves and closes the file.

Setting up a second network interface

If the Avaya CMS system has two network interfaces, you must set up the second network interface. The primary network interface was set up during the Solaris installation.

To set up a second network interface:

1. Enter:

   `vi /etc/hosts`

2. Add a new line in the **/etc/hosts** file for each ACD that will connect to this computer using TCP/IP. You must enter the IP address and the host name.

   The following example shows the recommended default IP addressing scheme for a second network interface. The host name for the second network interface is the Avaya CMS system hostname with “`_1`” as a suffix.

```
#
# Internet host table
#
127.0.0.1       localhost
192.168.2.1     cms   cms.tempdomain.net  loghost
192.168.2.2     switch1
192.168.2.6     switch2
192.168.2.108  cms-rsc
192.168.2.3     cms_1    #2nd network card
192.168.2.101   cmsterm1
192.168.2.102   cmsterm2
192.168.2.103  router
```

3. Press **Esc**. Then enter:

   ```
   :wq!
   ```

   The system saves and closes the file.

4. If you are not sure what the second network interface type is, enter the following command:

   T5120/T5220 only:

   ```
   prtconf -v|egrep "e1000g|network"
   ```

   T4-1 or x86 only:

   ```
   prtconf -v|egrep "igb|network"
   ```

The system displays a message that is similar to the following example for the SPARC platform:

```
network, instance #0

                dev_path=/pci@0/pci@0/pci@1/pci@0/pci@2/network@0:e1000g0
                dev_link=/dev/e1000g0

network, instance #1

                dev_path=/pci@0/pci@0/pci@1/pci@0/pci@2/network@0,1:e1000g1
                dev_link=/dev/e1000g1

network, instance #2

                dev_path=/pci@0/pci@0/pci@1/pci@0/pci@3/network@0:e1000g2
                dev_link=/dev/e1000g2

network, instance #3

                dev_path=/pci@0/pci@0/pci@1/pci@0/pci@3/network@0,1:e1000g3
                dev_link=/dev/e1000g3
```

Note:
Depending on the system type, the fourth or fifth column will display the network card slot number. The system may not display the primary network interface if the interface is integrated.

5. Create a new host name file for the second network interface by entering:

   vi /etc/hostname.*network_interfaceX*

   where ***network_interface*** is the type of network interface, and

   where ***X*** is the instance of the network interface.

   Example:

   On a Sun T5120/T5220, enter:

   `vi /etc/hostname.e1000g0`

   On a Sun T4-1 or x86, enter:

   `vi /etc/hostname.igb0`

6. Add a line to this new file with the host name you added to the **/etc/hosts** file.

   Example:

   ```
   cms_1
   ```

7. Press **Esc**. Then enter:

   :wq!

   The system saves and closes the file.

Editing the /etc/defaultrouter file

If the connection between the Avaya CMS system and the switch is going through a customer's network, you will have to set up a default network router.

To edit the **/etc/defaultrouter** file:

1. Enter:

   `vi /etc/defaultrouter`

   The system creates a default router file.

2. Add a line to this new file with the IP address for the default system router on the customer's network. This address must be obtained from the customer.

   Example:

```
192.168.2.254     router
```

3. Press **Esc**. Then enter:

   `:wq!`

   The system saves and closes the file.

4. Add the router information to the **/etc/hosts** file. See Editing the /etc/hosts file on page 81.

IPv6 Support on Solaris

1. Create a host name file for the IPv6 network interface by entering:

   `vi /etc/hostname6.network_interfaceX`

   where `network_interface` is the type of network interface, and `X` is the instance of the network interface.

   Example:

   On a Sun T5120/T5220, enter:

   `vi /etc/hostname6.e1000g2`

   On a Sun T4-1 or x86, enter:

   `vi /etc/hostname6.igb2`

2. Add a line to this new file with the IPv6 host name you added to the /etc/hosts file.

   Example:

```
cms_ipv6_1
```

3. Press **Escape**. Then enter:

   :wq!

   The system saves and closes the file.

Caveats to IPv6 use with AOM and Visual Vectors

AOM requires a system local IPv4 address to be available for the tool to work properly. The IPv4 address does not need to be visible outside of the CMS system.

Visual Vectors Server requires an IPv4 network address be available and used as the connection point for Visual Vectors client. The network may be hybrid IPv4/IPv6, but cannot be IPv6 exclusively.

Configuring the Avaya CMS software

The Avaya CMS software provides monitoring and recording of ACD calls and agents handling these calls, and the use of Vector Directory Numbers (VDNs) for these calls to measure call center performance.

This section includes the following topics:

- Prerequisites on page 86
- About the configuration methods on page 87
- Configuring Avaya CMS interactively on page 87
- Configuring Avaya CMS using a flat file on page 96

Prerequisites

Before you configure the Avaya CMS software, perform the following tasks:

- Verify that you are logged in as **root**.
- Verify that if TCP/IP is being used to connect to an ACD, the switch/LAN setup is done.

- Verify that all file systems are mounted.

About the configuration methods

You can choose either of the following ways to configure the Avaya CMS software:

- If you use the interactive option, the program automatically prompts you for the necessary information to configure the Avaya CMS software. For more information, see Configuring Avaya CMS interactively on page 87.
- If you use the flat file option, you edit a UNIX system flat file that contains the necessary information to set up the Avaya CMS software. When you execute the install program, the program runs in the background and uses the flat file data to configure Avaya CMS. For more information, see Configuring Avaya CMS using a flat file on page 96.

Configuring Avaya CMS interactively

To configure Avaya CMS interactively:

1. Enter:

   `cmssvc`

   The system displays the `Avaya Call Management System Services Menu`.
2. Enter the number associated with the `setup` option.
   a. If CMS is turned on, the system displays the following message and returns to the command prompt.

```
CMS needs to be turned off before invoking this command.
```

   Turn off cms and continue with step 3.

   b. If CMS is turned off, the system displays options for the set up type.

3. Select the option for the terminal.

   The system displays the following message:

```
Select the language for this server:

All languages are ISO Latin except Japanese. Selection of the
server language assumes that existing customer data is compatible.
(Upgrade from any ISO Latin language to any ISO Latin language or
from Japanese to Japanese is supported).

1) English
2) Dutch
3) French
4) German
5) Italian
6) Portuguese
7) Spanish
8) Japanese
Enter choice (1-8): (default: 1)
```

Note:
When the cmssvc `setup` command is running, no other CMSADM or cmssvc commands are allowed. Any attempt to run other CMSADM or cmssvc commands will be rejected, and the system will display the error message `“Please try later, setup is active”.`

Note:
If system setup has already been done, the program responds:

```
Warning!!! Setup has already been performed.
Running this command will remove all CMS data in the database.
Do you wish to proceed and re-configure CMS? (y/n): (default: n)
```

If the warning message is displayed, perform one of the following actions:

- Enter **`n`** to exit the setup.
- Enter **`y`** to continue with the setup.

4. Enter the number for the language to be used on this system.

5. The system displays the following options:

```
The input will be read from
      1) The terminal
      2) a flat file
Enter choice 1 or 2:
```

   Enter the appropriate choice.

a. If choice 2 is selected, the system displays the following message and returns to the command prompt.

```
***  The rest of this command is running in the background ***
```

b. If choice 1 is selected, the system initializes the customer Avaya CMS data. This can take up to 30 minutes. When finished, the system displays the following message:

```
## Initializing Customer CMS data . . .
.........................
Customer CMS data successfully initialized.
Creating database tables
.......
Enter a name for this UNIX system (up to 256 characters):
(default: cms3)
```

6. Enter the host name of the computer.

   This name was assigned during the factory installation procedures and is used by the TSC to maintain and identify this specific system.

   The system displays the following message:

```
Select the type of backup device you are using
   1) Tape
   2) Other
Enter choice (1-2):
```

   The following table lists the supported models of tape drives.

Tape drive	Tape cartridge	CMS computers
DAT 72	DDS compliant 170 meter 36/72-GB DAT cartridge 4 mm	Sun SPARC Enterprise T5120 Sun SPARC Enterprise T5220
LTO-4	820 meter 800 GB LTO cartridge 12.65 mm	Sun SPARC Enterprise T5120 Sun SPARC Enterprise T5220 Sun Netra X4270
LTO-5	846 meter 1.5 TB LTO cartridge 12.65 mm **Note**: LTO-4 cartridges can also be used in the LTO-5 drive.	Sun SPARC Enterprise T5120/T5220 Sun Netra X4270 Sun SPARC T4-1

7. The system displays the following message:

```
Enter the default backup device path: (default: /dev/null)
```

- If the tape option is selected, use the following steps to determine the device path of the tape drive:

  a. Insert a tape into the tape drive.

  b. In another xterm window, enter the following commands:

     `mt -f /dev/rmt/1c status`

     `mt -f /dev/rmt/0c status`

  The system will display a message similar to the following for the device that has the tape inserted:

```
HP DAT-72 tape drive:
   sense key(0x0)= No Additional Sense   residual= 0   retries= 0
   file no= 0   block no= 0
```

WARNING:
You cannot perform backups to `/dev/null`. The `/dev/null` device path allows customers who do not have a backup device to continue configuring CMS.

The `/dev/null` device path is not an option if type "Other" is selected. The CMS administrator needs to provide the path used for type "Other".

8. Enter the default backup device path.

   The system displays the following message:

```
Enter number of ACDs being administered (1-8):
```

9. Enter the number of ACDs to be administered. This number may be less than the number of ACDs authorized.

   The system displays the following message:

```
Information for ACD 1

Enter switch name (up to 20 characters):
```

10. Enter the name for the switch that is associated with ACD 1.

    The system displays a list of switch models.

11. Enter the number that represents the switch model that is associated with the ACD.

    Use the following table to determine the correct switch model. See *Avaya Call Management System Switch Connections, Administration, and Troubleshooting* for additional information.

    Switch model table

If the switch release is:	Then enter this switch model choice:
Release 2	Communication Mgr 2
Release 3.0	Communication Mgr 3.0
Release 3.1	Communication Mgr 3.1
Release 4	Communication Mgr 4/5
Release 5.0	Communication Mgr 4/5
Release 5.1	Communication Mgr 4/5
Release 5.2	Communication Mgr 5.2
Release 6.x	Communication Mgr 6.x

    If the switch supports vectoring and vectoring is authorized, the following message appears; otherwise, go to Step 14.

```
Is Vectoring enabled on the switch? (y/n):
```

12. Perform one of the following actions:

    - If vectoring is enabled on this switch, enter: **`y`**
    - If vectoring is not enabled on this switch, enter: **`n`**

    The following message appears if vectoring is enabled, the switch supports EAS, and EAS is authorized. If the message does not appear, go to Step 14.

```
Is Expert Agent Selection enabled on the switch? (y/n):
```

13. Perform one of the following actions:

    - If EAS is enabled on this switch, enter: **`y`**
    - If EAS is not enabled on this switch, enter: **`n`**

    The system displays the following message:

```
Does the Central Office have disconnect supervision? (y/n):
(default: y)
```

14. Perform one of the following actions:
    - If the Central Office has disconnect supervision, enter: **`y`**
    - If the Central Office does not have disconnect supervision, enter: **`n`**

    The system displays the following message:

```
If the Central Office has disconnect supervision, enter 0.  Otherwise,
ACD calls shorter than the Phantom Abandon Call Timer
value will be counted as abandoned.
Enter the Phantom Abandon Call Timer value in seconds (0-10):
```

15. Enter the Phantom Abandon Call Timer value.

    The system displays the following message:

```
Enter the local port assigned to switch. (1-64):
```

Note:
The standard Avaya CMS provisioning procedure is to set the local and remote port assignments equal to the switch processor channel assignment. For example, for switch processor channel 2, the remote and local port assignments would both be set to a value of 2.

16. Enter the local port or channel number on the switch.

    The system displays the following message:

```
Enter the remote port assigned to switch (1-64):
```

17. Enter the remote port or channel number on the switch.

    You must now select how the Avaya CMS platform transports messages to the switch.

    The system displays the following message:

```
Select the transport to the switch
1) TCP/IP
Enter choice (1-1):
```

18. Select TCP/IP.

    The system displays the following message:

```
Enter switch host name or IP Address:
```

19. Enter the host name or IP address of the switch that is connected to this ACD.

Note:
If you enter a host name that has not been added to the computer's **/etc/hosts** file, the system displays the following message:

```
Switch_name has not been administered in a DNS or
/etc/hosts file. The DNS or /etc/hosts file must be
corrected or the link to the switch will not work.
```

See Editing the /etc/hosts file on page 81 for more information about setting up the hosts file.

The system displays the following message:

```
Enter switch TCP port number (minimum-maximum):(default: 5001)
```

20. Press **Enter** to use the default TCP port number.

Note:
This number must match the port number administered on the switch.

The system displays the following message:

```
Number of splits/skills (0-Maximum):
```

21. Enter the number of splits/skills in this ACD.

The system displays the following message:

```
Total split/skill members, summed over all splits/skills
(0-Maximum):(default 500)
```

22. Enter the maximum number of split/skill members that will be logged into this ACD simultaneously, considering shift overlap.

- For non-EAS, sum all agent-split combinations, counting each split an agent will log into (maximum is 4) as a split member.
- For EAS, sum all agent-skill combinations that will be logged in at the same time. Count the maximum number of skills the supervisors expect to assign to each agent (maximum is 20) during a shift.

If it is not possible to sum the number of splits/skills for each agent, you can determine the capacity that is needed by multiplying the total number of agents by the average number of splits/skills per agent.

The system displays the following message:

```
Number of shifts (1-4):(default 1)
```

23. Enter the number of shifts.

    The system displays the following message:

    ```
    Enter the start time for shift 1 (hh:mmXM):(default 8:00 AM)
    ```

24. Enter the start time for shift 1.

    Example:

    `08:00AM`

    The system displays the following message:

    ```
    Enter the stop time for shift 1 (hh:mmXM) : (default 5:00 PM)
    ```

25. Enter the stop time for shift 1.

    Example:

    `05:00PM`

    The system displays the following message:

    ```
    Number of agents logged into all splits/skills during
    shift 1 (0-maximum):(default 5000)
    ```

26. Enter the number of agents logged in during the shift.

    Note:

    Repeat Steps 24 through 26 for the number of shifts entered in Step 23.

    When all shifts have been set up, the system displays the following message:

    ```
    Number of trunk groups (0-maximum):(default 500)
    ```

27. Enter the number of trunk groups that are associated with this ACD.

    The system displays the following message:

    ```
    Number of trunks (0-maximum):(default 1000)
    ```

28. Enter the number of trunks associated with this ACD.

    The system displays the following message:

    ```
    Number of unmeasured facilities (0-maximum):(default)
    ```

29. Enter the number of unmeasured trunk facilities that are associated with this ACD.

Note:
The recommended assignment per ACD for unmeasured facilities is 50% of the measured trunks.

If the switch supports call work codes, the system displays the following message:

```
Number of call work codes (minumum-maximum):(default 1000)
```

30. Enter the number of call work codes.

    If vectoring is enabled on the switch, that is if a `y` was entered in Step 12, the system displays the following message:

```
Enter number of vectors (0-maximum):(default 500)
```

31. Enter the number of vectors.

    The system displays the following message:

```
Enter number of VDNs (0-maximum):(default 4000)
```

32. Enter the number of VDNs.

    The program repeats Steps 10 through 31 for each ACD that you entered in Step 9.

    After you define the last ACD, the system displays the following message:

```
Updating database.

Creating database tables
.......

Computing space requirements and file system space
availability.

Setup completed successfully.
```

Note:
If the setup determines that you do not have enough file space, the system displays the following warning message:

```
Failed to find sufficient file space for CMS data.

WARNING: You do not currently have sufficient file space for your
existing CMS data. At this point you should turn on CMS, go to the
“Data Storage Allocation” screen, verify/modify the
administration, and go to the “Free Space Allocation” screen and
verify your available free space.

Setup completed with warnings.
```

33. To verify that the installation completed successfully, enter:

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

    All failure messages are logged in this file. The Avaya CMS software is successfully set up when the system displays a message similar to the following:

    ```
    Setup completed successfully <data/time>
    ```

    You may edit this file and add comments about the packages that were installed or authorized.

34. Perform one of the following actions:

    - If you need to install additional CMS-related feature packages such as Forecasting or External Call History, go to Installing feature packages on page 102.
    - If you are not installing any other feature packages, perform the following procedure:

        a. Enter:

        ```
        cmssvc
        ```

        The system displays the `Avaya Call Management System Services Menu`.

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

        c. Enter the number associated with the `Turn on CMS` option.

Configuring Avaya CMS using a flat file

To configure Avaya CMS using a flat file, you must edit a copy of the **cms.inst.skl** file and start the install program.

Important:
This procedure is not necessary if you already performed the Avaya CMS configuration interactively.

This section includes the following topics:

- Creating the flat file on page 96
- Example of a flat file on page 97
- Using the flat file on page 100

Creating the flat file

To configure Avaya CMS with a flat file:

1. Change to the Avaya CMS installation directory by entering:

   ```
   cd /cms/install/cms_install
   ```

2. Make a copy of the Avaya CMS installation file by entering:

   `cp cms.inst.skl cms.install`

3. Change permissions on the copied Avaya CMS installation file by entering:

   `chmod 644 cms.install`

4. Edit the copied Avaya CMS installation file by entering:

   `vi cms.install`

   The file contains a series of questions and value ranges for the ACD configuration.

Note:
When selecting a switch model in the file, refer to the Switch model table on page 91.

5. Enter the appropriate values for your configuration. The entries must be added on the blank lines after each question. For more information, see Example of a flat file on page 97.

CAUTION:
Use the computer's host name for the UNIX system name. The computer's host name was assigned during the factory installation.

6. Press **Esc**. Then enter:

   `:wq!`

   The system saves and closes the file.

Example of a flat file

The following section shows an example of a flat file.

```
# Enter a name for this UNIX system (up to 256 characters):
cuckoo
# Select the type of backup device you are using
#    1) 40.0+ Gbyte tape
# Enter choice (1-1):
1
# Default backup device paths based on device type:
# Device                         Default backup path
# 40.0+ Gbyte tape               /dev/rmt/0c
# Enter the default backup device path:
/dev/rmt/0c
# Enter number of ACDs being administered (1-8):
1
# The following information is required per ACD:
# Information for ACD 1:
# Enter switch name (up to 20 characters):
switch1
# Select the model of switch for this ACD
#    1) Communication Mgr 2
#    2) Communication Mgr 3.0
#    3) Communication Mgr 3.1
#    4) Communication Mgr 4/5
#    5) Communication Mgr 5.2
#    6) Communication Mgr 6.0
# Enter choice (1-6):
4
# Is Vectoring enabled on the switch? (y/n):
y
# Is Expert Agent Selection enabled on the switch? (y/n):
y
# Does the Central Office have disconnect supervision? (y/n):
y
# If the Central Office has disconnect supervision, enter 0.  Otherwise,
# ACD calls shorter than the Phantom Abandon Call Timer
# value will be counted as abandoned.
# Enter the Phantom Abandon Call Timer value in seconds (0-10):
0
# Enter the local port assigned to switch (1-64):
1
# Enter the remote port assigned to switch (1-64):
1
# TCP/IP available on DEFINITY R9/R10 and later switches.
# Select the transport to the switch
#    1) TCP/IP
# Enter choice (1-1):
1
# Skip the next two questions if you did not enter choice TCP/IP.
# These are used for TCP/IP connections only.
# If a host name is entered, the host name must be administered in a DNS or
# /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:
switch1
# Enter switch TCP port number (5001-5999):
5003
# Maximum number of splits/skills based on switch type:
# Release(s)                                    Value
# Communication Mgr 2/Communication Mgr 3.0      2000
# Communication Mgr 3.1/Communication Mgr 4/5    2000
# Communication Mgr 5.2                          2000
# Communication Mgr 6.0                          8000
# Number of splits/skills (0-Maximum):
1000
# Maximum number of split/skill members based on switch type:
# Release(s)                                    Value
# Communication Mgr 2/Communication Mgr 3.0     60000
# Communication Mgr 3.1                         60000
# Communication Mgr 4/5/Communication Mgr 5.2  100000
# Communication Mgr 6.0                        100000
# Total split/skill members, summed over all splits/skills (0-Maximum):
100000
# Number of shifts (1-4):
1
# Enter the start time for shift 1 (hh:mmXM):
 8:00am
```

```
# Enter the stop time for shift 1 (hh:mmXM):
 5:00pm
# Number of agents logged into all splits/skills during shift 1 (1-Maximum):
100000
# Maximum number of trunk groups based on switch type:
# Release(s)                                    Value
# Communication Mgr 2/Communication Mgr 3.0      2000
# Communication Mgr 3.1/Communication Mgr 4/5    2000
# Communication Mgr 5.2/Communication Mgr 6.0    2000
# Number of trunk groups (0-Maximum):
2000
# Maximum number of trunks based on switch type:
# Release(s)                                    Value
# Communication Mgr 2/Communication Mgr 3.0      8000
# Communication Mgr 3.1                          8000
# Communication Mgr 4/5/Communication Mgr 5.2   12000
# Communication Mgr 6.0                         12000
# Number of trunks (0-Maximum):
8000
# Maximum number of unmeasured trunks:
# Release(s)                                    Value
# Communication Mgr 2/Communication Mgr 3.0      4000
# Communication Mgr 3.1                          4000
# Communication Mgr 4/5/Communication Mgr 5.2    6000
# Communication Mgr 6.0                          6000
# Number of unmeasured facilities (0-Maximum):
4000
# Minimum number of call work codes based on switch type:
# Release(s)                                    Value
# Communication Mgr 2/Communication Mgr 3.0         1
# Communication Mgr 3.1/Communication Mgr 4/5       1
# Communication Mgr 5.2/Communication Mgr 6.0       1
# Maximum number of call work codes based on switch type:
# Release(s)                                    Value
# Communication Mgr 2/Communication Mgr 3.0      1999
# Communication Mgr 3.1/Communication Mgr 4/5    1999
# Communication Mgr 5.2/Communication Mgr 6.0    1999
# Number of call work codes (Minimum-Maximum):
500
# Maximum number of vectors based on switch type:
# Release(s)                                    Value
# Communication Mgr 2                             999
# Communication Mgr 3.0/Communication Mgr 3.1    2000
# Communication Mgr 4/5/Communication Mgr 5.2    2000
# Communication Mgr 6.0                          8000
# Enter number of vectors (0-Maximum):
500
# Maximum number of VDNs based on switch type:
# Release(s)                                    Value
# Communication Mgr 2/Communication Mgr 3.0     20000
# Communication Mgr 3.1/Communication Mgr 4/5   20000
# Communication Mgr 5.2                         20000
# Communication Mgr 6.0                         30000
# Enter number of VDNs (0-Maximum):
10000
```

```
# Information for ACD 2:........
```

Note:
The file repeats the preceding statements for ACDs 2 through 8. Enter data for only the required number of ACDs.

Using the flat file

To use the flat file to configure Avaya CMS:

1. Enter **`cd /`** to change to the root directory.
2. Enter:

   `cmssvc`

   The system displays the `Avaya Call Management System Services Menu`.
3. Enter the number associated with the `setup` option.

   If setup has been done previously, the system displays the following message:

```
Warning!!! Setup has already been performed.
Running this command will remove all CMS data in the database.
Do you wish to proceed and re-configure CMS? (y/n): (default: n)
```

4. Enter: **`y`**

   The system displays the following message:

```
Select the language for this server:

All languages are ISO Latin except Japanese. Selection of the
server language assumes that existing customer data is compatible.
(Upgrade from any ISO Latin language to any ISO Latin language or
from Japanese to Japanese is supported).

1) English
2) Dutch
3) French
4) German
5) Italian
6) Portuguese
7) Spanish
8) Japanese
Enter choice (1-8): (default: 1)
```

5. Enter the number associated with the language that is used on the system.

   The system displays the following message:

```
The input will be read from
  1) the terminal
  2) a flat file
Enter choice (1-2):
```

6. Enter the number associated with the `flat file` option.

   The system displays the following message:

```
*** The rest of this command is running in the background ***
```

7. Verify that the installation completed successfully by entering:

   `tail -f /cms/install/logdir/admin.log`

   The `-f` option in the `tail` command updates the console as messages are written to the **admin.log** file. All failure messages are logged in this file. The Avaya CMS software is successfully set up when you see a message similar to the following:

```
Setup completed successfully <data/time>
```

   You can edit this file and add comments about the packages that were installed or authorized.

8. Press **Delete** to exit the **`tail -f`** command.

9. Choose one of the following:

   - If you need to install additional CMS-related feature packages (Forecasting or External Call History), go to Installing feature packages on page 102.
   - If you are not installing any other feature packages, do the following to turn on the Avaya CMS software:

     a. Enter:

        `cmssvc`

        The system displays the `Avaya Call Management System Services Menu`.

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

     c. Enter the number associated with the `Turn on CMS` option.

Important:
If no additional configuration of the Avaya CMS software is needed, see Setting the Informix configuration parameters for Avaya CMS on page 124.

Installing feature packages

Customers can install Avaya CMS feature packages if the packages have been authorized during Avaya CMS setup. You can contact the National Customer Care Center (1-800-242-2121), or consult with your product distributor or representative to additional feature packages, see Configuring Avaya CMS authorizations on page 67 for additional information.

This section includes the following topics:

- Prerequisites on page 102
- Installing the Forecasting package on page 102
- Installing the External Call History package on page 104
- Installing Avaya CMS Supervisor Web on page 108
- Installing the Avaya Visual Vectors Server software on page 112

Prerequisites

Before you begin the installation procedures, perform the following tasks:

- Verify that you are logged in as **root**.
- Verify that all file systems are mounted.

Installing the Forecasting package

To install the Forecasting package:

1. Enter:

   ```
   cmssvc
   ```

   The system displays the `Avaya Call Management System Services Menu`.
2. Enter the number associated with the `auth_display` option.

   The system lists the current authorizations.
3. Verify that the system is authorized to install the Forecasting package.

Note:
If Forecasting is not authorized but should be, see Configuring Avaya CMS authorizations on page 67.

4. Enter:

   cmsadm

   The system displays the Avaya Call Management System Administration Menu.

Note:
Different options may be displayed in the Avaya Call Management System Administration Menu depending on the current version of Avaya CMS on your system.

5. Enter the number associated with the pkg_install option.

   The system displays the following message:

```
The CMS Features that can be installed are
  1) forecasting
  2) external call history
Enter choice (1-2) or q to quit:
```

Note:
The pkg_install option menu displays only those feature packages that are authorized but not yet installed. The Forecasting package does not require the Avaya CMS software to be off during the installation. If Forecasting is added at a later date, the Avaya CMS software can be left on.

6. Enter the number that corresponds to the forecasting package.

   The system displays the following message:

```
Installation was successful

Forecasting package installed.

At this point you should go to the “Free Space Allocation Screen”
and verify that you have enough space for Forecasting on each ACD.
If there is not enough space allocated, then modify your existing
free space.
```

   If the installation fails, the system displays the following message:

```
Forecasting package installation failed.
```

7. If you are not installing any other feature packages, do the following to turn on the Avaya CMS software:

   a. Enter: **cmssvc**

      The system displays the Avaya Call Management System Services Menu.

   b. Enter the number associated with the run_cms option.

   c. Enter the number associated with the Turn on CMS option.

8. Go to the `Free Space Allocation` window that is located in the Avaya CMS System Setup subsystem, verify that there is enough space for Forecasting on each ACD, and make any necessary modifications.

   For more information about Free Space Allocation, see *Avaya Call Management System Release 16 Administration*.

9. Verify that the installation completed successfully by entering:

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

   If the Forecasting package was successfully installed, the system displays the following message:

```
  .
  .
Forecasting package installed (date/time)
```

   You can edit this file in order to add comments about the packages that were installed or authorized.

Installing the External Call History package

To install the External Call History (ECHI) package:

> **Important:**
> Once the External Call History package is installed, you can no longer access any call record data directly from the Avaya CMS software. For more information, see *Avaya Call Management System Call History Interface*.

1. Verify that:
   - A separate computer is available for the storage and reporting of call records.
   - The storage computer and the Avaya CMS system are administered in UNIX-to-UNIX copy (UUCP). If the storage machine is not running the UNIX operating system, then the storage machine must use a DOS version of UUCP.
   - The Avaya CMS software is off and the IDS software is on.

2. Enter:

   `cmssvc`

   The system displays the `Avaya Call Management System Services Menu`.

3. Enter the number associated with the `auth_display` option.

   The system displays the current authorizations. Different authorizations may be displayed depending on the version of Avaya CMS on your system.

4. Verify that the system is authorized for the ECHI package. If ECHI is not authorized but should be, see Configuring Avaya CMS authorizations on page 67.

5. Enter:

   cmsadm

   The system displays the `Avaya Call Management System Administration Menu`.

6. Enter the number associated with the `pkg_install` option.

   The system displays the following message:

```
The CMS Features that can be installed are
  1) forecasting
  2) external call history
Enter choice (1-2) or q to quit:
```

Note:
The system displays only feature packages that are authorized but not yet installed.

7. Enter the number that corresponds to the ECHI package (in this example, `2`).

   The system displays the following message:

```
Enter name of computer to which to send call records
(up to 256 characters)
```

8. Enter the name of the computer where call records will be collected.

   The system displays the following message:

```
Enter full path of the program to transmit the external call
history files: (default: /cms/dc/chr/uucp_copy)
```

9. Press **Enter**.

   The system displays the following message:

```
Enter full path of the program to check the external call history
file transmission: (default: /cms/dc/chr/uucp_check)
```

10. Press **Enter**.

    The system displays the following message:

```
Enter password for nuucp login on computer (up to 8 characters)
```

11. Enter the password for nuucp on the receiving computer that was administered in uucp.

    The system displays the following message:

    ```
    Enter CMS port for connection to computer (s_pdevxxx):
    ```

12. Enter the Avaya CMS port that is administered for the Call History Reporting machine.

    The system displays the following message:

    ```
    Select a speed for this connection
    1) 19200
    2) 38400
    Enter choice (1-2):
    ```

13. Enter the speed that the connection between the Avaya CMS system and the call history reporting system.

    The system displays the following message:

    ```
    Number of call segments to buffer for ACD xxxxx (0-99999):
    ```

14. Enter the number of call records to be held in the buffer if the Call History machine cannot accept the data. Repeat this step for each administered ACD.

    Select whether ECHI will use the extended ECH record format.

    ```
    Start ECH in the on or off state: (default off)
    ```

15. Select whether ECHI will start in the on or off state (default is off). If the receiving system has not yet been set up, the recommended state is off. ECHI can be turned on at a later date with the `run_pkg` option in the `Avaya Call Management System Administration Menu`.

    The system displays the following message:

    ```
    Computing space requirements and file system space availability.

    External Call History package installed.
    ```

    If the setup determines that you do not have enough file space, you will get the following warning message:

    ```
    Failed to find sufficient file space for CMS data.

    WARNING: You do not currently have sufficient file space for your
    existing CMS data. At this point you should turn on CMS, go to the
    “Data Storage Allocation” screen, and verify/modify the
    administration, or go to the “Free Allocation” screen and verify/
    modify your existing free space.

    External call history package installed with warnings.
    ```

16. Verify that the installation completed successfully by entering:

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

    If the ECHI package was installed successfully, the system displays the following message:

    ```
    External Call History package installed (date/time)
    ```

    You may edit this file in order to add comments about the packages that were installed or authorized.

17. If you are not installing any other feature packages, do the following to turn on the Avaya CMS software:

    a. Enter:

       `cmssvc`

       The system displays the `Avaya Call Management System Services Menu`.

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

    c. Enter the number associated with the `Turn on CMS` option.

    For more information about the ECHI feature, see *Avaya Call Management System Call History Interface*.

Installing Avaya CMS Supervisor Web

The Avaya CMS Supervisor Web software is installed on the same server as the Avaya CMS software. Avaya CMS Supervisor Web is web based and allows customers to access CMS reports from a wider range of hardware platforms.

1. Verify the Avaya Call Management System software disc for your specific platform architecture (SPARC or x86), is loaded in the disc drive.
2. To install the CMS Supervisor Web package, enter:

   `/usr/sbin/pkgadd -d /cdrom/cdrom0 cmsweb`

   The system displays the following messages:

```
Processing package instance <cmsweb> from </cdrom/cms_<platformtype_XX.xxxx.x>

CMS Web Interface(sparc/x86) webXX.xx.x
Copyright (c) 2011 Avaya Inc.
All Rights Reserved


The selected base directory </opt/cmsweb> must exist before installation is
attempted.

Do you want this directory created now [y,n,?,q]
```

3. Enter: **y**

   The system displays the following messages:

```
Using </opt/cmsweb> as the package base directory.

## Processing package information.
## Processing system information.
   1 package pathname is already properly installed.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <cmsweb> [y,n,?]
```

4. Enter: **y**

   The system installs the new **CMS Supervisor Web** package.

⚠ **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.

5. To start the CMS WebClient, enter:

```
cmsweb start
```

Certificate Management

A security certificate is needed to encrypt communication between browsers and CMS Supervisor Web server. Upon first installation of the **cmsweb** package, a self-signed certificate is automatically generated by the installation process based on the host name and domain name of the host server. You can view the URL/Common Name used in this certificate by the following command:

```
# /opt/cmsweb/bin/showcrt.sh
```

The URL/Common Name should be used to access the CMS Supervisor Web GUI from the browser. If the URL does not appear correct due to the network and host setup, use the following command to change it:

```
#  /opt/cmsweb/bin/chgcert.sh
```

The above command prompts for the new URL. The default value for this command is your host name and domain name (if the domain name is configured on your host). Press **Enter** to accept the default or type in your preferred URL.

Generating and installing a customer certificate for the cmsweb server

1. Generate a new key store and a new key.

   a. Create a new custom directory for the certificate on the CMS server.

   ```
   # mkdir /opt/cmsweb/cert/custom
   ```

   b. Change the current directory to the newly created directory.

   ```
   # cd /opt/cmsweb/cert/custom
   ```

c. Generate a new key and key store.

```
# keytool -genkey -alias cmsweb -keyalg RSA -keysize 2048
  -keystore cmsweb.jks
```

This command prompts for a password and other information. The password must be `cmsweb`. The first and last name must be the domain name of the CMS server.

For example:

```
# keytool -genkey -alias cmsweb -keyalg RSA -keysize 2048
  -keystore cmsweb.jks
```

The system output and the user entries for the questions are as follows:

```
Enter keystore password: cmsweb
Re-enter new password: cmsweb
What is your first and last name?
  [Unknown]:  tweety.dr.avaya.com
What is the name of your organizational unit?
  [Unknown]:  CMS
What is the name of your organization?
  [Unknown]:  Avaya
What is the name of your City or Locality?
  [Unknown]:  Westminster
What is the name of your State or Province?
  [Unknown]:  Colorado
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=tweety.dr.avaya.com, OU=CMS, O=Avaya, L=Westminster, ST=Colorado,
C=US correct? Y

Enter key password for <cmsweb>
        (RETURN if same as keystore password): <ret>
```

2. Generate a certificate request.

```
# keytool -certreq -keyalg RSA -alias cmsweb -file certreq.csr
  -keystore cmsweb.jks
```

The system output and user entry are as follows:

```
Enter keystore password:  cmsweb
```

3. Use the certificate request in file `certreq.csr` to get a certificate from the certificate authority (CA) of your choice.

4. Install the root certificate from the CA.

   a. Copy and paste the CA root certificate into a file, for example, `root.cert`.

b. Import the root certificate.

```
# keytool -import -alias root -keystore cmsweb.jks -trustcacerts
  -file root.cert
```

The system output and user entry are as follows:

```
Enter keystore password: cmsweb
```

Sometimes the CA also issues an intermediate CA certificate. If the CA issues an intermediate certificate, import the intermediate CA certificate also.

c. Copy and paste the intermediate certificate into a file, for example, `intermediate.cert.`

d. Import the intermediate certificate.

```
# keytool -import -alias intermediate -keystore cmsweb.jks
  -trustcacerts -file intermediate.cert
```

The system output and user entry are as follows:

```
Enter keystore password: cmsweb
```

5. Install the new certificate.

a. Copy and paste the new certificate into a file, for example, `cmsweb.cert`.

b. Import the certificate.

```
# keytool -import -alias cmsweb -keystore cmsweb.jks
  -trustcacerts -file cmsweb.cert
```

The system output and user entry are as follows:

```
Enter keystore password: cmsweb
```

6. Stop the cmsweb server.

```
# cmsweb stop
```

7. Copy the key store in the correct location.

```
# cp /opt/cmsweb/cert/custom/cmsweb.jks /opt/cmsweb/cert
```

8. Start the cmsweb server.

```
# cmsweb start
```

Installing the Avaya Visual Vectors Server software

The Visual Vectors Server software is installed on the same server as the Avaya CMS software. The Visual Vector Server software supports Visual Vectors client software installed on PC workstations. Using the client software, administrators can change certain properties of call center entities, as well as create and edit vectors, assign Vector Directory Numbers (VDNs) to vectors, and set VDN Skill Preferences.

To install the Avaya Visual Vectors Server software:

1. Log into the system as **root**.
2. Install the Avaya CMS R16.3 Software Installation disc.
3. Enter:

   `pkgadd -d /cdrom/cdrom0 LUfaas`

   If this is the first time that Visual Vectors has been installed, the system displays the following message:

   ```
   Processing package instance <LUfaas> from </cdrom/untitled>

   Visual Vectors Server Software
   (sparc) vvsXX.X
   ......
   ......
   ......
   Do you want this directory created now [y,n,?,q]
   ```

4. Enter: **`y`**

   The system displays the following message:

   ```
   Using </cms/aas> as the package base directory.

   ## Processing package information.
   ## Processing system information.
   ## Verifying package dependencies.
   ## Verifying disk space requirements.
   ## Checking for conflicts with packages already installed.

   The following files are already installed on the system and are
   being used by another package:

   * /cms/aas <attribute change only>
   * - conflict with a file which does not belong to any package.

   Do you want to install these conflicting files [y,n,?,q]
   ```

5. Enter: **`y`**

   The system displays the following message:

```
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with
super-user permission during the process of installing this
package.

Do you want to continue with the installation of <LUfaas> [y,n,?]
```

Note:
The system may display a message about creating the user ID aasadmin. If the system displays this message, enter: **`y`**

6. Enter: **`y`**

   The system displays the following message:

```
Installing Visual Vectors Server Software as <LUfaas>

## Installing part 1 of 1.
..........
..........
..........
Installation of <LUfaas> was successful.
```

7. Enter:

   `setupaas`

   The system displays the `Avaya Visual Vectors System Services Menu`.

```
Avaya Visual Vectors Server System Services Menu

Select a command from the list below.

  1) init_vvs     Setup the initial configuration
  2) run_vvs      Turn VVS on or off
  3) auth_display Display simultaneous VVS logins
  4) auth_set     Change simultaneous VVS logins
  5) backup       Backup vector steps and layout files
  6) restore      Restore vector steps and layout files

Enter choice (1-6) or q to quit:
```

Note:
Ignore the message “aasadmin does not exist” as the aasadmin user will be created during the installation process.

8. Enter the number associated with the `init_vvs` option.

   The system displays the following message:

```
This version of VVS functions only with CMS.

CMS name used : cms3
Maximum concurrent VVS logins[1-100](q to quit):
```

9. Enter the number of required concurrent Visual Vector users.
10. Enter:

    `eject cdrom`

Setting up the remote console

This section describes how to set up and redirect the remote console port using the Solaris software package. The remote console allows the TSC or COE to dial in and perform maintenance.

This section includes the following topics:

- The remote console access port on page 114
- Administering the remote console port on page 115
- Using the remote console port on page 116

Note:
For the x86 and T4-1 systems, the console cannot be redirected to show bootup information as T5120/T5220 systems can.

The remote console access port

The port that is used for remote console access differs, depending on the hardware platform:

Hardware platform	Port A	Port B	Port 0
Sun Enterprise T5120	Remote console	None	None

Hardware platform	Port A	Port B	Port 0
Sun Enterprise T5220	Remote console	None	None
Sun Netra X4270 with DigiPort USB Serial converter	None	None	Remote console

Note:
On T4-1, remote access and alarming are supported only by SAL.

Administering the remote console port

To administer the remote console port on the back of the Avaya CMS system:

1. Remove the current port administration by entering:

   `/cms/install/bin/abcadm -r ttyX`

   where ***X*** is **a,** or **b,** or **0**.

   The system displays the following message:

```
ttyX is currently set to be incoming

Are you sure you want to change it? [y,n,?]
```

2. Enter: **y**

   The system displays the following message:

```
ttyX administration removed
```

3. Enter the following to administer the remote console port:

   `/cms/install/bin/abcadm -i -b 9600 ttyX`

   where ***X*** is **a,** or **b,** or **0**.

   The system displays the following message:

```
ttyX set to incoming port 9600 baud
#
```

   The remote console port has been administered.

Using the remote console port

To use the remote console port functions on an Avaya CMS system:

1. Dial in from the remote console to the remote console modem on the Avaya CMS system and log in as **root**.
2. Remove the port monitor by entering:

   `/cms/install/bin/abcadm -r ttyX`

   where ***`X`*** is **`a`** or **`b`**.

   The system displays the following message:

   ```
   ttyX is currently set to be incoming

   Are you sure you want to change it? [y,n,?]
   ```

3. Enter: **`y`**

   The system displays the following message:

   ```
   ttyX administration removed
   ```

4. Redirect the console to the remote console port by entering:

   `/cms/install/bin/abcadm -c -b 9600 ttyX`

   where ***`X`*** is **`a`** or **`b`**.

   Note:
   Systems on the x86 and T4-1 platform do not support console redirection.

   The system displays the following message:

   ```
   This change requires a reboot to take affect

   Are you ready to reboot? [y,n,?]
   ```

5. Enter: **`y`**

   The system displays the following message at the remote console:

   ```
   done
   desktop auto-start disabled
   Proceding to reboot.
   ```

   The system will automatically reboot, and the remote console port will come up as the console.

   The following occurs:

- The system begins to shut down.
- Shut down, reset and reboot messages appear on the local console.
- When the system starts to come back up, the local console goes blank.
- The system boot diagnostics are displayed on the remote console.
- After the system reboots, a `console login:` prompt is displayed on the remote console.

6. Log into the remote console as **root**.

   CAUTION:
   You may lock yourself from using the console locally or remotely if you enter **Ctrl+D** or **`exit`** from the remote console to exit the system without first redirecting control back to the local console.

7. Redirect the console back to the local console by entering:

   `/cms/install/bin/abcadm -c local`

   The system displays the following message:

```
Console set to local

This change requires a reboot to take affect

Are you ready to reboot? [y,n,?]
```

8. At the remote console, enter: **`y`**

   The following occurs:

   - The system begins to shut down.
   - Shutdown, reset, and reboot messages appear on the remote console.
   - When the system starts to come back up, the system boot diagnostics are displayed on the local console.
   - After the system reboots, the `console login:` prompt is displayed on the remote console.
   - The login screen is displayed on the local console.

9. Log into the local console as **root**.
10. Log into the remote console as **root**.

    Control of the console port is redirected from the remote console back to the local console.

    If you experience problems with the remote console, see Diagnosing dial-In access problems on page 252 for additional information.

Setting up the Alarm Origination Manager

Use this section to set up the Alarm Origination Manager (AOM) on the Avaya CMS system. The AOM feature is available only for Avaya CMS systems in the US and Canada with a current maintenance warranty agreement in effect.

This section includes the following topics:

- Prerequisites on page 118
- Setting up the AOM configuration files on page 118
- Creating an AOM test alarm on page 122

Prerequisites

Before you set up AOM, perform the following tasks:

- The Avaya CMS Supplemental Services packages must be installed and set up.
- A “Product ID” number must be obtained from the Avaya CMS database administration group. (Avaya CMS technical support personnel must contact the database group at 800-248-1111, extension 07425 and provide them with the customer IL number.)

Setting up the AOM configuration files

There are two ways to set up the AOM configuration files. You can set up the configuration files automatically using the command **`aom_tool`**, or you can use the older manual procedure.

To set up the AOM configuration files automatically:

1. Log in as `root2` or `cmssvc`.

   Note:
   Use the appropriate password, available only to Avaya CMS technical support personnel, to log in as `root2` or `cmssvc`.

2. You must install Avaya CMS Supplemental Services for alarming. To verify that Avaya CMS Supplemental Services is installed, enter:

   ```
   pkginfo -x | grep LU
   ```

3. Verify the output list contains the following packages:

```
LUahl                               Network Administration History Log
LUaot                               Alarm Origination Manager
LUim                                Avaya(TM) Installation Manager
LUorbutil                           1A1 Orbix Wrappers
```

4. Choose one of the following options to set up the AOM configuration files:
   - To set up the AOM configuration files automatically, continue with Step 5.
   - To set up the AOM configuration files manually, continue with Step 9.
5. To get command line usage help for the AOM tool, run the following commands:

   cd /cms/toolsbin

   ./aom_tool ?
6. To run the AOM tool enter the following commands:

   cd /cms/toolsbin

   ./aom_tool

   Messages similar to the following are displayed:

```
Checking /etc/hosts is linked to /etc/inet/hosts                   [sPassed
Checking /etc/nsswitch.conf                                        [sPassed
Welcome to Avaya CMS Alarm Origination main menu (v1.16.3.7).

     1) Send a test alarm
     2) Send a test alarm with a different ARS code
     c) Configure AOM
     q) Quit
```

7. Select the option associated with **Configure AOM.**

   Follow the prompts to set up the AOM configuration files.
8. Continue with Step 22.
9. Check the version of Avaya CMS installed on the system, enter:

   pkginfo -x cms

   The system displays the version of Avaya CMS that is installed.

```
cms   Avaya(TM) Call Management System
      (sparc) r16.Xxx.y
```

10. Record the Avaya CMS version information which will be used to update the `prodSetup.cfg` file in Step 15.

11. Identify the communications port used by the system modem, enter:

    ```
    tty
    ```

    The system displays the communications port which is one of `/dev/term/a`, `/dev/term/b`, or `/dev/term/0`.

12. Record the port information which will be used to update the `sysSetup.cfg` file in Step 20.

13. Change to the AOM admin directory, enter:

    ```
    cd /opt/cc/aot/data/admin
    ```

14. Edit the fields in the `prodSetup.cfg` file, enter:

    Note:
    Make a backup copy of the `prodSetup.cfg` file before making any changes.

    ```
    vi prodSetup.cfg
    ```

    The system displays the contents of the `prodSetup.cfg` file.

15. Edit the fields in the `prodSetup.cfg` file to be similar to the following example:

    ```
    Product|NumberInstances|ServiceVehicle|Enabled|
    TEST   |1              |r1v0          |1      |
    CMS    |1              |rxxxxx.x      |1      |
    ```

    where *rxxxxx.x* is the Avaya CMS version number you recorded in Step 10.

16. Write and save the `prodSetup.cfg` file, enter

    ```
    :wq!
    ```

17. Modify the `sysSetup.cfg` file.

    Note:
    Make a backup copy of the `sysSetup.cfg` file before making any changes.

    ```
    vi sysSetup.cfg
    ```

    The system displays the `sysSetup.cfg` file:

    - If the system is a T5120,T5220, or x86 platform, continue with Step 18.
    - If the system is a T4-1 platform, continue with Step 20.

18. Update the following three fields in the `sysSetup.cfg` file with the appropriate customer information:

    - `ProductID` - This is the first field in the `sysSetup.cfg` file. It is a unique system identifier obtained from the database administration group. See Prerequisites on page 118.
    - `TelephoneNum` - This is the fifth field in the `sysSetup.cfg` file. It is the telephone number of the Initialization and Administration (INADS) alarm receiver: 800-535-3573. The number must be preceded by the modem “dial tone” command and followed by all

digits required for an outgoing call. For example, if a “9” is required to gain outside access, the entry in the TelephoneNum field would be:

ATDT918005353573

- ModemPort - This is the eighth field in the sysSetup.cfg file. It is the modem port that you identified in Step 12, expressed in numeric form (ttya = 1 and ttyb = 2). If tty0, enter cua/0 in this field.

19. Continue with Step 21.
20. To set up a Virtual NIU on a T4-1 platform, you need to modify the sysSetup.cfg file as follows:
    - ModemType: This field is set to socket.
    - DialString: This field is the IP address of the SAL/SSG to which CMS sends alarms.
    - ModemPort: This field is the network port on which the SAL/SSG receives alarms. The network port for CMS is 5108.

    An example of the file using the virtual NIU is as follows:

Product ID	ModemType	DialString	Exp1	TelephoneNum	Exp2	ReturnStr	ModemPort	BaudRate	Enabled
3000001234	socket	10.11.12.13	OK	ATDT18003453293	CONNECT	XXXXXXXXXX	5108	9600	1

21. Write and save the sysSetup.cfg file, enter:

    :wq!

22. Set the Test variable by entering:

    export PRODUCT_TYPE=TEST

23. Stop and restart AOM by entering the following commands:

    aom stop

    aom start

24. Continue with Creating an AOM test alarm on page 122.

Creating an AOM test alarm

To create a test alarm to verify that AOM is properly set up:

1. Log in as **root2** or **cmssvc**
2. Enter:

   ```
   cd /opt/cc/aot/bin
   ```
3. Enter the following commands:

   ```
   . ./aom_env
   ```

   ```
   env | grep AOM_SH
   ```

   If the environment is set correctly, the system displays the following line of output:

   ```
   AOM_SH=/usr/bin/aom
   ```
4. Send the test alarm by entering:

   ```
   ./log_error -e 30001
   ```
5. Log off the system. Wait about 5 minutes to give the system time to send the alarm before logging back in.
6. Enter:

   ```
   cd /opt/cc/aot/data/log
   ```
7. Enter:

   ```
   cat alarm_log
   ```

   When the test succeeds, the system displays a message at the end of the log file similar to the following example:

   ```
   07/04/00 14:17:30|30001|TEST|1|TEST_ALARM|MINOR|2|Call Attempt(1)|06/28/00
   +73935305-5:
   07/04/00 14:17:30|30001|TEST|1|TEST_ALARM|MINOR|2|Call Attempt(2)|06/28/00
   +74149665-5:
   07/04/00 14:17:30|30001|TEST|1|TEST_ALARM|MINOR|2|Positive Acknowledge|
   07/04/00 14:17:30|
   ```

   In addition, technical support personnel should find an open case for this test alarm in the CMSALM folder in the MAESTRO case system.

Starting the Avaya Visual Vectors Server software

To start the Avaya Visual Vectors Server software:

1. Stop and restart AOM by entering the following commands:

   `aom stop`

   `aom start`

2. Enter:

   `setupaas`

   The system displays the `Avaya Visual Vectors System Services Menu`.

```
Avaya Visual Vectors Server System Services Menu

Select a command from the list below.

  1) init_vvs     Setup the initial configuration
  2) run_vvs      Turn VVS on or off
  3) auth_display Display simultaneous VVS logins
  4) auth_set     Change simultaneous VVS logins
  5) backup       Backup vector steps and layout files
  6) restore      Restore vector steps and layout files

Enter choice (1-6) or q to quit:
```

3. Enter the number associated with the `run_vvs` option.

   The system displays the following message:

```
1) Turn VVS On
2) Turn VVS Off

Enter choice (1-2) or q to quit:
```

4. Enter the number associated with the `Turn VVS On` option.

Note:
The *first* time you turn on Visual Vectors after a new installation, the software could take up to 30 minutes to turn on. The actual length of time will depend on the number of vectors administered on your ACDs.

Setting the Informix configuration parameters for Avaya CMS

The IDS configuration parameters for Avaya CMS are automatically optimized for system performance during the installation of Informix.

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

   `pkginfo -x cms`

   If CMS is installed, the system displays the following:

```
cms  Avaya(TM) Call Management System
     (sparc) r16.Xxx.y
```

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

   `/cdrom/cdrom0/cmssolasg.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.

Removing Access Security Gateway

To remove Access Security Gateway (ASG) from your CMS server, run the following command as `root`:

```
/etc/asg/uninstall_asgsolaris.sh
```

Turning the system over to the customer

This section describes how to test the Avaya Call Management System (CMS) software to ensure that the application is working properly before the system is turned over to the customer.

Perform these procedures after:

- Completing the initial computer installation and Avaya CMS setup
- Completing an Avaya CMS software package upgrade

This section includes the following topics:

- Prerequisites on page 127
- Verifying the system date and time on page 128
- Forwarding Avaya CMS system warning messages on page 128
- Checking free space allocation on page 129
- Testing the remote access port on page 131
- Testing the ACD link on page 135
- Assigning customer passwords on page 136
- Repeat this procedure for each customer login. on page 136
- Testing the Avaya CMS software on page 136
- Finalizing the on-site installation on page 139

Prerequisites

Before you begin the procedures described in *Turning the system over to the customer*, the technicians must:

- Locate the two sets of backup tapes (the original set from the factory that were delivered with the new system and the set created by provisioning during installation) and set these tapes to write-protect mode
- Connect the Avaya CMS system to the switch
- Translate the switch with the Avaya CMS feature enabled
- Connect the switch to an active link

Verifying the system date and time

Verify that the Solaris operating system time and the current local time are the same.

Follow the procedures in Changing the system date and time on page 191. Then continue with Checking free space allocation on page 129.

Restoring EEPROM values

Note:
This only applies to T5120/T5220 and T4-1 systems.

Restore EEPROM variables auto-boot? and fcode-debug? to their original values.

Set auto-boot? to true, enter:

```
eeprom auto-boot?=true
```

Set fcode-debug? back to it's original setting, enter:

```
eeprom fcode-debug?=<Orig_fcode-debug?>
```

where `Orig_fcode-debug?` is the original `fcode-debug?` setting documented in Step 8 of the section Booting a T5120/T5220 system to the Solaris 10 DVD on page 21 or Booting a T4-1 system to the Solaris 10 DVD on page 23.

Forwarding Avaya CMS system warning messages

The CMS system can forward warning messages to specific customer e-mail addresses. If you do not enable the CMS system to forward warning messages, the messages will remain in the CMS system root e-mail account.

⚠ **Important:**
To use this feature, you must have Avaya Professional Services install either the Admin Paging or Supervisor Paging packages. Contact Avaya support for more information.

To forward CMS system warning messages:

1. Obtain the e-mail addresses of any customer CMS administrators who want to receive the warning messages.

2. Enter:

   ```
   cd /
   ```

3. Create the file for the e-mail addresses by entering:

   ```
   vi /.forward
   ```

4. Enter an e-mail address on a single line in the file. You can enter more than one e-mail address but each e-mail address must be on a single line as shown in the following example:

   ```
   admin1@company.com
   admin2@company.com
   admin3@company.com
   ```

5. Save and quit the file by pressing **Esc** and entering:

   ```
   :wq!
   ```

6. Change the file permissions by entering the following command:

   ```
   chmod 600 /.forward
   ```

Checking free space allocation

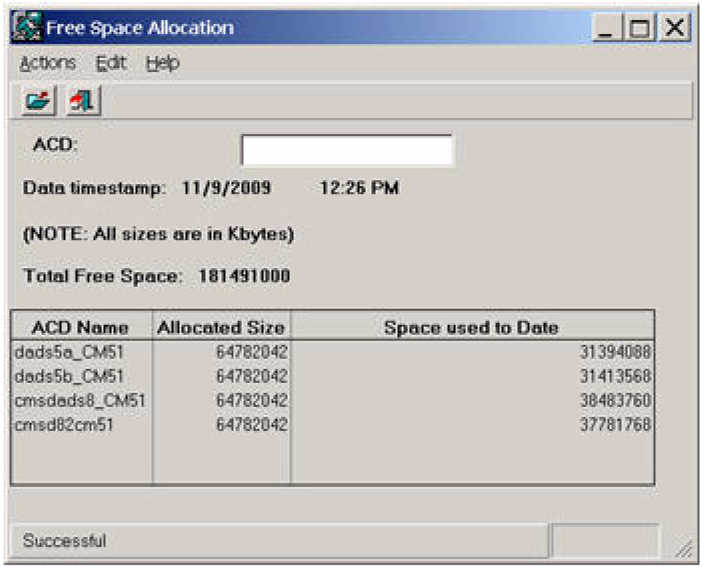
To check free space allocation:

1. Go to the **Free Space Allocation** window that is located in the CMS System Setup subsystem.

2. Verify that the amount of available space is positive for each ACD.

   For more information about free space allocation, see *Avaya Call Management System Release 16 Administration*.

   Example:



ACD:

Data timestamp: 11/9/2009 12:26 PM

(NOTE: All sizes are in Kbytes)

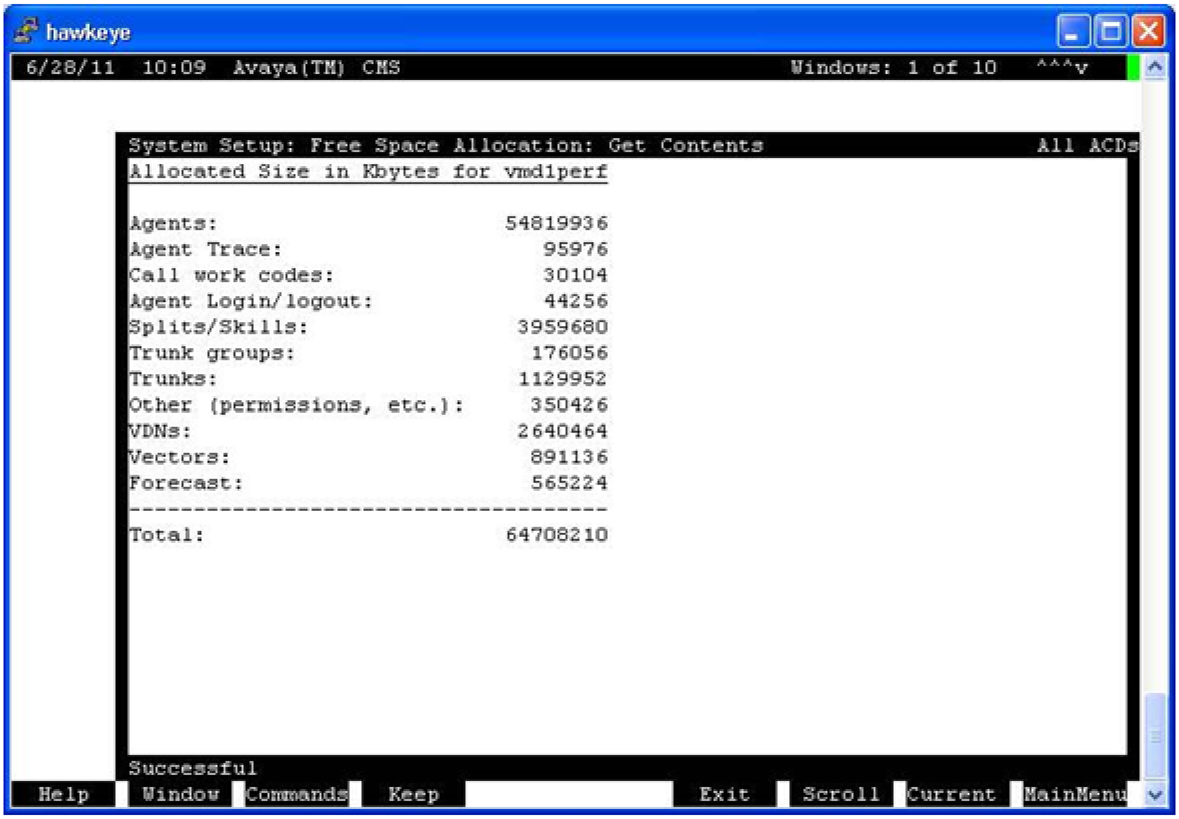
Total Free Space: 181491000

ACD Name	Allocated Size	Space used to Date
dads5a_CM51	64782042	31394088
dads5b_CM51	64782042	31413568
cmsdads8_CM51	64782042	38483760
cmsd82cm51	64782042	37781768

Successful

If the `Total Free Space:` field shows that there is not enough space available and you must modify data storage allocation.

Example of the **Get Contents** screen.



```
6/28/11  10:09  Avaya(TM) CMS                          Windows: 1 of 10   ^^^v

        System Setup: Free Space Allocation: Get Contents                 All ACDs
        Allocated Size in Kbytes for vmd1perf

        Agents:                          54819936
        Agent Trace:                        95976
        Call work codes:                    30104
        Agent Login/logout:                 44256
        Splits/Skills:                    3959680
        Trunk groups:                      176056
        Trunks:                           1129952
        Other (permissions, etc.):         350426
        VDNs:                             2640464
        Vectors:                           891136
        Forecast:                          565224
        -------------------------------------
        Total:                           64708210

        Successful
  Help   Window  Commands   Keep                Exit   Scroll  Current  MainMenu
```

Testing the remote access port

You must test the remote access port to verify that the TSC or COE can connect to the Avaya CMS system. The remote access port allows the TSC or COE to perform remote maintenance. The port that is used for remote console access differs depending on the hardware platform. See the following table for more information.

Hardware platform	Port A	Port B	Port 0
Sun Enterprise T5120	Remote console	None	None

Hardware platform	Port A	Port B	Port 0
Sun Enterprise T5220	Remote console	None	None
Sun Netra X4270 with DigiPort USB Serial converter	None	None	Remote console

Note:
On T4-1, remote access and alarming are supported only by SAL.

This section includes the following topics:

- Redirecting the console to the remote console (T5120/T5220 systems only) on page 132
- Redirecting the console back to the local console on page 134

Redirecting the console to the remote console (T5120/T5220 systems only)

To redirect the console to the remote console:

1. Dial in from the remote console to the remote console modem and log in as **root**.
2. At the remote console, enter:

   /cms/install/bin/abcadm -r tty*X*

   where ***X*** is **a** or **b**.

   The system displays the following message:

```
ttyX is currently set to be incoming

Are you sure you want to change it? [y,n,?]
```

3. At the remote console, enter: **y**

   The system displays the following message:

```
ttyX administration removed
```

4. Check the speed of the modem by entering:

   /cms/install/bin/abcadm -k

Note:
All remote access ports have a default speed of 9600 bps.

5. Redirect the console to the remote console port by entering:

   `/cms/install/bin/abcadm -c -b 9600 tty`*`X`*

   where ***`X`*** is **`a`** or **`b`**.

   The system displays the following message:

```
This change requires a reboot to take affect

Are you ready to reboot? [y,n,?]
```

6. At the remote console, enter: **`y`**

   The system displays the following message at the remote console:

```
done
desktop auto-start disabled
Proceeding to reboot.
```

   The system automatically reboots, and the remote console port comes up as the console.

   The following occurs:

   - The system begins to shut down.
   - Shut down, reset and reboot messages appear on the local console.
   - When the system starts to come back up, the local console goes blank.
   - The system boot diagnostics are displayed on the remote console.
   - After the system reboots, a `console login:` prompt is displayed on the remote console.

7. Log into the remote console as **root**.

   The local console is blank.

CAUTION:
You may lock yourself from using the console locally or remotely if you enter **Control+D** or exit from the remote console to exit the system without first redirecting control back to the local console.

Redirecting the console back to the local console

To redirect the console back to the local console:

1. Enter:

   `/cms/install/bin/abcadm -c local`

   The system displays the following message:

```
Console set to local

This change requires a reboot to take affect

Are you ready to reboot? [y,n,?]
```

2. Enter: **`y`**

   The following occurs:

   - The system begins to shut down.
   - Shutdown, reset, and reboot messages appear on the remote console.
   - When the system starts to come back up, the system boot diagnostics are displayed on the local console.
   - After the system reboots, the `console login:` prompt is displayed on the remote console.
   - The login screen is displayed on the local console.

3. Log into the local console as **root**.
4. Log into the remote console as **root**.

   Control of the console port is redirected from the remote console back to the local console.

   If you have problems with the remote access port, see Diagnosing dial-In access problems on page 252.

Testing the ACD link

After the Avaya CMS software has been installed or upgraded, the on-site technician must test the link from the Avaya CMS system to the switch that is using the Automatic Call Distribution (ACD) feature.

To test the ACD link:

1. Verify that:
   - The Common Desktop Environment (CDE) is active
   - Avaya CMS is on.
2. In one of the windows at a console, log into the system by using a CMS administrator's login ID (**su - cms**). Enter the correct password if prompted.
3. Enter:

   ```
   cms
   ```
4. Enter the correct terminal type.

   The CMS Main Menu is displayed.

   The CMS Main Menu has indicators that show whether the link to the ACD is active. The link indicator consists of the carets (\/ and /\) at the right side of the banner line. There should be one caret for each ACD, and all should be pointed up (^).

   Example:

   If you have four ACDs, the link indicator should look like this: ^^^^, which means that all four ACDs are up and operating.
5. Select **Maintenance** from the CMS Main Menu.

   The system displays the **Maintenance** menu.
6. Select **Connection Status** from the **Maintenance** menu.

   The **Connection Status** window displays the following information:
   - The name of the ACD
   - Whether the application is in data transfer
   - Whether the session is in data transfer
   - Whether the connection is operational
   - The date, time, and any errors
7. Press the **Exit** screen-labeled key (SLK) once.

Assigning customer passwords

This section describes how the customer assigns passwords to each of its logins on the Avaya CMS system. The customer must assign passwords to each of the following logins:

- root
- cms
- Any other administration logins that have been added for the customer

To assign a password to a customer login:

1. Log in as **root**.
2. At the system prompt, have the customer enter:

   `passwd` ***`login`***

   where ***`login`*** is root, cms, and so on.

   The system displays the following message:

```
New password:
```

3. Have the customer enter the new password.

   The system displays the following message:

```
Re-enter new password:
```

4. Have the customer enter the password again.

   Note:
   The technician should *not* know these passwords.

5. Repeat this procedure for each customer login.

Testing the Avaya CMS software

After the Avaya CMS software has been installed or upgraded, the on-site technician must test the Avaya CMS software to verify its sanity.

To test the Avaya CMS software:

1. Verify that:
   - The Common Desktop Environment (CDE) is active
   - Avaya CMS is on.

2. Test the Real-Time Reports subsystem.
   a. Enter

      `CMS`

      The system displays the `CMS Main Menu`.
   b. Select **Reports**.
   c. Select **Real-time**.
   d. Select **Split/Skill**.
   e. Select **Split Status** or **Skill Status**.
   f. Verify that the **Split/Skill Status Report** input window is displayed.
   g. Enter a valid split number in the `Split:` or `Skill:` field.
   h. Select the **Run** action list item, and run the report.
   i. Verify that the **Split** or **Skill Status Report** window is displayed.
   j. If the switch link is not operating, the report fields are blank and the status line reads **Switch link down**.
   k. Press the **Commands** SLK.
   l. Select **Print window** to send the report to the printer.
   m. Look at the message line near the bottom of the window, and verify that there is a confirmation message about sending the report to the printer.
   n. Verify that the report was printed by checking the printer for the report.
   o. Return to the CMS Main Menu screen by pressing the **Exit SLK** twice.
3. Test the Historical Reports subsystem.
   a. On the CMS Main Menu, select **Reports**.
   b. Select **Historical**.
   c. Select **Split/Skill**.
   d. Select **Status**.
   e. Verify that the **Split/Skill Status Report** Input window is displayed.
   f. Enter a valid split number in the `Split/Skill:` field.
   g. Enter **`-1`** in the `Date:` field.
   h. Select the **Run** action list item, and run the report.
   i. Verify that the report window is displayed and that the information is displayed in the appropriate fields.

Note:
If no historical data exists, the fields in the report window are blank.

   j. Return to the `CMS Main Menu` by pressing the **Exit SLK** twice.

4. Test the Dictionary subsystem by doing the following from the CMS Main Menu.
   a. On the CMS Main Menu select **Dictionary**.
   b. Select **Login Identifications**.
   c. Enter an asterisk (*****) in the `Login ID:` field.
   d. Select the **List all** action list item. The system lists all the login IDs.
   e. Verify that the logins are displayed.

   Note:
   On a new system, the fields are blank.

   f. Return to the CMS Main Menu by pressing the **Exit SLK** twice.
5. Test the Exceptions subsystem.
   a. On the CMS Main Menu select **Exceptions**.
   b. Select **Real-time Exception Log**.
   c. Verify that the window is displayed.

   Note:
   For a new installation, this window may be blank.

   d. Return to the **CMS Main Menu** by pressing the **Exit SLK** once.
6. Test the Call Center Administration subsystem.
   a. On the CMS Main Menu select **Call Center Administration**.
   b. Select the **Call Work Codes** option.
   c. Press **Enter**.
   d. Select the **List all** action list item, and list all the call work codes currently defined.
   e. Verify that the displayed information is correct.

   Note:
   On a new system, the fields may be blank.

   f. Return to the CMS Main Menu by pressing the **Exit SLK** twice.
7. Test the Custom Reports subsystem.
   a. On the CMS Main Menu select **Custom Reports**.
   b. Select **Real-time**. The system lists the names of the custom reports.
   c. Verify that the names of existing custom reports are listed. If there are no reports, you receive a message saying the submenu is empty.
   d. Return to the CMS Main Menu by pressing the **Exit SLK** once.
8. Test the User Permissions subsystem.

a. On the CMS Main Menu select **User Permissions**.

b. Select **User Data**.

c. Verify that the **User Data Input** window is displayed.

d. Return to the CMS Main Menu by pressing the **Exit SLK** once.

9. Test the System Setup subsystem.

   a. On the CMS Main Menu select **System Setup**.

   b. Select **CMS state**.

   c. Verify that CMS is operating in the Multi-user mode.

   d. Return to the CMS Main Menu by pressing the **Exit** SLK once.

10. Test the Maintenance subsystem.

    a. On the CMS Main Menu select **Maintenance**.

    b. Select the **Printer Administration** option.

    c. Enter a valid printer name in the `CMS printer name:` field.

    d. Select the **List all** action list item. The system lists the printer parameters.

    e. Verify that the printer has been administered correctly.

    f. Return to the CMS Main Menu by pressing the **Exit SLK** twice.

11. If the Graphics feature package has been enabled, test the Graphics subsystem.

    a. On the CMS Main Menu select **Graphics**.

    b. Verify that a Real-time Graphics screen can be accessed.

    c. Return to the CMS Main Menu by pressing the **Exit SLK** once.

    d. At each CMS terminal, log in as **cms** and enter the correct terminal type to verify that the terminals are working properly. To log off, select the `Logout` option from the `CMS Main Menu`.

    If any of the steps in this test fail, see Avaya CMS error logs on page 240, Common error messages on page 265, or Recognizing new hardware devices on page 239. If you encounter a problem that you cannot solve, escalate the problem through normal procedures.

Finalizing the on-site installation

This section contains the final steps that the on-site technician must perform before turning the system over to the customer.

Before turning the system over to the customer, perform the following steps:

1. Back up the system. Follow the procedures outlined in CMSADM backup on page 161.

   ⚠ **CAUTION:**
   Use a new set of backup tapes for this CMSADM file system backup. Do NOT use the original set of factory backup tapes or provisioning backup tapes. Make sure that the customer has enough tapes for the new backup.

2. Back up the customer's historical data by doing a full maintenance backup. You can do these backups within Avaya CMS using the `Maintenance: Back Up Data` window.

   For more information about maintenance backups, see *Avaya Call Management System Release 16 Administration*.

3. Set up alarming. For more information about the AOM tool, see Setting up the Alarm Origination Manager on page 118.
4. Give the customer all of the Avaya CMS documentation, the software discs, and the tape backups (including the original set from the factory, and the set created by provisioning).
5. Have the customer record their logins and passwords. The technician should NOT know these login passwords.
6. Give the passwords, backup tapes, and software to the customer's CMS administrator.

   ⚠ **CAUTION:**
   For system security and recovery, the CMS administrator should store passwords, Informix serial numbers, key license information, and the tape backups in a secure location.

Maintaining the Avaya CMS software

This section provides the procedures for maintaining the Avaya Call Management System (CMS) software.

This section includes the following topics:

- Using the CMSADM menu on page 141
- Using the CMSSVC menu on page 153
- The Avaya CMS backups on page 161
- CMSADM backup on page 161
- Backing up the CMS system on page 163
- Changing the system date and time on page 191
- Working with Solaris patches on page 193
- Working with Avaya CMS patches on page 198
- Adding and removing users from password aging on page 202
- Maintaining the chkDisks crontab on page 205
- Report Query Status on page 206

Using the CMSADM menu

This section describes how to use the options in the `Avaya Call Management System Administration Menu` (`CMSADM menu`). The CMSADM menu is intended for use by the CMS administrator.

This section includes the following topics:

- CMSADM menu functions on page 142
- Accessing the CMSADM menu on page 142
- Using acd_create on page 143
- Using acd_remove on page 145
- Using backup on page 146
- Using pkg_install on page 146
- Using pkg_remove on page 147

- Using run_pkg on page 147
- Using run_ids on page 147
- Using run_cms on page 148
- Using passwd_age on page 148
- Using dbaccess on page 150

CMSADM menu functions

The following list shows the tasks that the CMS administrator can perform from the `CMSADM menu`:

- Define a new Automatic Call Distribution (ACD)
- Remove an ACD
- Back up the file systems to tape
- Install or remove a feature package
- Turn a feature package on or off
- Turn the IDS software on or off
- Turn the Avaya CMS software on or off
- Turn password aging on or off
- Change Informix DB access permissions

Accessing the CMSADM menu

To access the CMSADM menu:

1. Log in as **root**.

2. Enter **cmsadm**.

   The system displays the **CMSADM** menu.

```
Select a command from the list below.
   1) acd_create   Define a new ACD
   2) acd_remove   Remove all administration and data for an ACD
   3) backup       Filesystem backup
   4) pkg_install  Install a feature package
   5) pkg_remove   Remove a feature package
   6) run_pkg      Turn a feature package on or off
   7) run_ids      Turn Informix Database on or off
   8) run_cms      Turn Avaya CMS on or off
   9) passwd_age   Set password aging options
  10) dbaccess     Change Informix DB access permissions
Enter choice (1-10) or q to quit:
```

Note:
Your system may display different options in the CMSADM Menu depending on the version of CMS you installed.

Important:
When the cmssvc **setup** command runs on your system, it rejects all attempts to run other **cmsadm** or **cmssvc** commands and displays the error message "Please try later, setup is active".

Using acd_create

Enter the acd_create option to define a new ACD. The information you enter here for each ACD is the same as the setup option of the CMSSVC menu.

Note:
You must purchase and authorize the ACD before you add it to the CMS system.

Prerequisites:

1. Before you define a new ACD, you must turn off the CMS software:
   a. Enter **cmsadm.**

      The system displays the **CMSADM** menu.

   b. Enter the number associated with the **run_cms** option.
   c. Enter the number to turn off the Avaya CMS software but leave the IDS software on.
2. Enter **cmsadm.**

   The system displays the **CMSADM** menu.

3. Enter the number associated with the **acd_create** option.

   The system selects the next available ACD for creation. For example, if two ACDs are already active, the system selects ACD 3.

4. At the prompts, enter the following information for the new ACD:

   - Switch name
   - Switch model (release)
   - Vectoring enabled on the switch (if authorized): y or n
   - Expert Agent Selection (EAS) enabled on the switch (if authorized): y or n
   - Central Office has disconnect supervision: y or n
   - Local port assigned to the switch
   - Remote port assigned to the switch
   - Transport method used to connect to the switch (TCP/IP)
   - The hostname or IP address and TCP port
   - Number of splits/skills
   - Total split/skill members, summed over all splits/skills
   - Number of shifts
   - Start and stop times of all shifts
   - Number of agents logged in to all splits/skills across all shifts
   - Number of trunk groups
   - Number of trunks
   - Number of unmeasured (trunk) facilities
   - Number of call work codes
   - Number of vectors if vectoring is enabled on the switch
   - Number of Vector Directory Numbers (VDNs), if Vectoring is enabled on the switch

   After you enter the required information, the program displays the following message:

```
Updating database.

Computing space requirements and file system space
availability.

ACD <name> (X) created successfully.
```

5. To turn on the CMS software:

   a. Enter **`cmsadm.`**

      The system displays the **CMSADM** menu.

   b. Enter the number associated with the **run_cms** option.

   c. Enter the option to turn on the Avaya CMS software.

Using acd_remove

Use the `acd_remove` option to remove an existing ACD.

Note:
Before you remove the master ACD, you must designate another ACD as the master.

To designate a different ACD as the master:

1. On the main CMS menu, select **System Setup - CMS State**.
2. Use the **Tab** key to go to the **Master ACD** field and enter a new name.
3. Press **Enter** to go to the action list and select `Modify`.
4. Return to the main menu and select `Logout`.

To remove an ACD:

1. Verify that data collection is off for all ACDs.
2. Turn off the Avaya CMS software:
   a. Enter **`cmsadm.`**

      The system displays the **CMSADM** menu.

   b. Enter the number associated with the **run_cms** option.

   c. Enter the option to turn off the Avaya CMS software but leave the IDS software on.
3. Enter **`cmsadm.`**

   The system displays the **CMSADM** menu.
4. Enter the number associated with the **acd_remove** option.
5. Enter the number (`1-8`) that corresponds with the ACD that you want to remove.

   The system displays the following message:

```
All administration and historical data for this ACD will be
DELETED.
Do you want to continue and delete all data for this ACD? (y/n):
```

6. Enter: **`y`**

   The system displays the following message:

   ```
   Removal of data for this ACD started in the background.
   A completion message will be logged in /cms/install/logdir/
   admin.log.
   ```

7. Since the ACD is removed in the background, you can turn the Avaya CMS software on before the removal is complete. To turn the Avaya CMS software on, perform the following procedure:

   a. Enter **`cmsadm.`**

      The system displays the **CMSADM** menu.

   b. Enter the number associated with the **run_cms** option.

   c. Enter the option to turn on the Avaya CMS software.

Using backup

Use the **backup** option to back up your file system. This option does not back up Avaya CMS data.

Note:
To back up Avaya CMS data, you must perform a full maintenance backup in addition to the CMSADM backup. Refer to *Avaya CMS Administration* for more information on performing a full maintenance backup and CMSADM backup.

Using pkg_install

Use the `pkg_install` option to install a feature package.

1. Enter **`cmsadm`**.

   The system displays the **CMSADM** menu.

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

   The system displays the following message:

   ```
   The CMS Features that can be installed are
     1) forecasting
     2) external call history
   Enter choice (1-2) or q to quit:
   ```

Note:
The system only displays authorized feature packages that are yet to be installed.

3. Enter the number associated with the feature package that you want to install.

Using pkg_remove

Use the `pkg_remove` option to remove a feature package. This procedure removes all files and database items associated with the feature package.

> ⚠ **CAUTION:**
> Be careful when removing a package. All features and data associated with that package are also removed.

1. Enter **`cmsadm`**.

   The system displays the **CMSADM** menu.

   Note:
   CMS must be turned off before packages can be removed.

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

   The system displays a list of Avaya CMS features that can be removed.

3. Enter the number associated with the feature package that you want to remove.

   The system displays a message indicating the feature is removed.

Using run_pkg

Use the `run_pkg` option to turn a feature package on or off.

1. Enter **`cmsadm`**.

   The system displays the **CMSADM** menu.

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

   The system displays a list of Avaya CMS features.

3. Enter the number associated with the feature package that you want to turn on or off.

   The system displays the status of the feature.

Using run_ids

Use the `run_ids` option to turn IDS on or off.

1. Enter **`cmsadm`**.

   The system displays the **CMSADM** menu.

2. Enter the number associated with the `run_ids` option.
3. Perform one of the following actions:
   - To turn on IDS, enter: **1**
   - To turn off IDS, enter: **2**

Using run_cms

Use the `run_cms` option to turn the Avaya CMS software on or off.

1. Enter **cmsadm**.

   The system displays the **CMSADM** menu.
2. Enter the number associated with the `run_cms option`.
3. Perform one of the following actions:
   - To turn the Avaya CMS software on, enter: **1**
   - To turn the Avaya CMS software off, but leave IDS running, enter: **2**
   - To turn both the Avaya CMS software and IDS software off, enter: **3**

Using passwd_age

Use the `passwd_age` option to turn password aging on or off. If password aging is on, the system prompts the user to enter a new password after a predetermined time interval has passed. Password aging is off by default.

⚠ **CAUTION:**
If you have any third party software or Avaya Professional Services Organization (PSO) offers, do not turn on password aging. Contact the National Customer Care Center at 1-800-242-2121, or consult your product distributor or representative to ensure that password aging does not disrupt any additional applications.

The `passwd_age` option effects the passwords of all Avaya CMS users and regular UNIX users. When password aging is on, the system modifies the Solaris policy file **/etc/default/passwd**. The passwords of all Avaya CMS users that use the **/usr/bin/cms** shell and all UNIX users start aging. If password aging is on when a new user is added, the user's password begins to age as soon as a password is entered for that account.

Avaya recommends that you exclude specific users before turning password aging on in order to avoid additional password administration. If you need to prevent the aging of a specific user's password, see Adding and removing users from password aging on page 202 and Troubleshooting password aging on page 239.

Important:
Non-CMS users such as **root**, **root2,** or **Informix** do not age.

Password aging does not function on an Avaya CMS system that uses a NIS, NIS+, or LDAP directory service. Avaya does not support use of NIS, NIS+, or LDAP with CMS. If you are using NIS, NIS+, or LDAP under permissive use, contact your network administrator. The passwords need to be aged from the server running the directory service.

To use the `passwd_age` option:

1. Enter **`cmsadm`**.

   The system displays the **CMSADM** menu.

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

   The system displays the following message:

```
1) Turn on password aging
2) Turn off password aging
3) Change password aging interval
    or q to quit:  (default 1)
```

Note:
The system also displays a message indicating that password aging is off, or the current password aging schedule. Enter **`q`** at any point to exit the password aging options.

3. Perform one of the following actions:

   - To turn password aging on:

     a. Enter: **`1`**

        The system displays the following message:

```
Enter Maximum number of weeks before passwords expire (9 default):
```

     b. Enter the number of weeks before passwords expire and the system prompts users to enter a new password. The range is from 1 to 52 weeks.

   - To turn password aging off:

     a. Enter: **`2`**

        The system displays the following message:

```
Turn off password aging for all CMS users (yes default):
```

     b. Perform one of the following actions:

        – To turn password aging off, enter: **`yes`**

        – To leave password aging on, enter: **`no`**

- To change the password aging interval:

  a. Enter: `3`

     The system displays the following message:

```
Passwords are currently expiring every X weeks
Enter Maximum number of weeks before passwords expire (9 default):
```

  b. Enter the number of weeks before passwords expire and the system prompts users to enter a new password. The range is from 1 to 52 weeks.

Using dbaccess

Use dbaccess to limit which CMS logins have ODBC/JDBC access to the CMS database. The CMS database has open access permissions as a standard feature which allows permission to any CMS login, connecting to the CMS server through ODBC/JDBC, to view any CMS table. No action is required if all CMS logins are allowed open access to the CMS database.

The dbaccess utility does not provide the ability to control which tables the CMS login has access to, or which ACD data the CMS login can view. The process of setting the secure database access is performed in two parts. First, all CMS login-ids that are allowed CMS database access must be members of the UNIX group dbaccess. Second, you must execute the dbaccess option under the CMSADM menu.

Note:
Adding a single CMS login to the dbaccess group disables open access permissions for all users who are not members of the dbaccess group.

1. You need to add each CMS login, allowing ODBC/JDBC access to the CMS database, to the UNIX group dbaccess. To add CMS logins to the dbaccess group, enter:

   `usermod -G dbaccess` *`cmslogin`*

   Where *cmslogin* is the user-id of the specific CMS login to be placed in the group. You must execute the usermod command for each CMS login for which you want to provide CMS database access.

2. To determine which logins are in the dbaccess group, enter:

   `cat /etc/group | grep dbaccess`

3. Open the **Avaya Call Management System Administration** menu. Enter:

   `cmsadm`

   The system displays the **Avaya Call Management System Administration** menu.

4. Select the **dbaccess** option. The system displays the following message:

```
Begin CMS DB Access Permissions changes
grant resource to "public";

Your CMS database currently has public access permissions to all resources. Do you
wish to revoke this access and only grant access to specific CMS users? [y,n,?]
```

5. Enter: **y**

   The process continues. The system displays the following messages:

```
Please wait while CMS Informix Database permissions are changed.
revoke resource from public;
revoke connect from public;
grant connect to cms;
grant connect to cmssvc;
Revoke resource from public on CMS database.
Please wait while connect permissions are granted for requested users
grant connect to <cmslogin>;
grant connect to <cmslogin>;
.
.
.
Changes to CMS DB Access Permissions finished.
```

Note:
The output always displays one grant connect message per CMS login, including logins already in the dbaccess group with connect permissions.

After the changes are complete, you may use the CMS logins to run ODBC/JDBC clients and access the CMS database.

To remove ODBC/JDBC access permissions for CMS logins, first remove them from the UNIX dbaccess group then run dbaccess from the *Avaya Call Management System Administration* menu.

6. Remove ODBC/JDBC access permissions for CMS logins from the UNIX dbaccess group. Enter:

   `usermod -G “”` *`cmslogin`*

7. Open the **Avaya Call Management System Administration** menu. Enter:

   `cmsadm`

   The system displays the **Avaya Call Management System Administration** menu.

8. Select the **dbaccess** option. The system displays the following message:

```
Begin CMS DB Access Permissions changes
Please wait while connect permissions are granted for requested users
grant connect to  <cmslogin>;
.
.
.
Changes to CMS DB Access Permissions finished.
```

   The UNIX dbaccess group information is reset to only provide access permissions to members remaining in the UNIX dbaccess group.

   Perform the Steps 9 through 11 to remove all the CMS logins from the UNIX dbaccess group and restore “open access” permissions to all the CMS logins.

9. Run the usermod command for each CMS login in the dbaccess group. Enter:

   usermod -G “” *cmslogin1*

   usermod -G “” *cmslogin2*

   usermod -G “” *cmslogin3*

10. Open the **Avaya Call Management System Administration** Menu. Enter:

    cmsadm

    The system displays the **Avaya Call Management System Administration** menu.

11. Select the **dbaccess** option. The system displays the following message:

```
Begin CMS DB Access Permissions changes

No CMS user ids are in UNIX group dbaccess.
If you proceed, the CMS database will
be set to public permissions access for all resources.
Do you really want to do this? [y,n,?]
```

12. Enter: **y**

    The process restores public permissions to the CMS database. The system displays messages similar to the following:

```
Please wait while CMS Informix Database permissions are set to public.
grant resource to public;
revoke connect from cms;
revoke connect from cmssvc;
Grant resource to public on CMS database.
Changes to CMS DB Access Permissions finished.
```

Using the CMSSVC menu

This section describes how to use the options of the `Avaya Call Management System Services Menu` (`CMSSVC menu`). The `CMSSVC menu` is for use primarily by Avaya authorized services personnel.

This section includes the following topics:

CMSSVC menu functions

Avaya authorized services personnel can perform the following tasks from the CMSSVC menu:

- Display Avaya CMS authorizations
- Authorize Avaya CMS feature packages and capacities
- Turn the IDS software on or off
- Turn the Avaya CMS software on or off
- Set up the initial Avaya CMS configuration
- Display switch information
- Change switch information
- Install an Avaya CMS patch
- Back out an installed Avaya CMS patch

- Install all Avaya CMS patches
- Back out all installed Avaya CMS patches

Accessing the CMSSVC menu

1. Log in as **root**.
2. Enter **`cmssvc`**.

   The system displays the **CMSSVC** 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) patch_inst   Install a single CMS patch from CD
  9) patch_rmv    Backout an installed CMS patch
  10) load_all     Install all CMS patches found on CD
  11) back_all     Backout all installed CMS patches from machine
Enter choice (1-11) or q to quit:
```

Note:
When the CMSSVC **`setup`** command is running, any attempt to run other **`cmsadm`** or **`cmssvc`** commands will be rejected, and the system will display the error message:

```
Please try later, setup is active
```

Note:
Different options may be displayed in the `CMSSVC Menu` depending on the current version of Avaya CMS on your system.

Using auth_display

To use the `auth_display` option to display Avaya CMS authorizations:

1. Enter **`cmssvc`**.

   The system displays the **CMSSVC** menu.

2. Enter **1** to select `auth_display`.

   The system displays the Avaya CMS version and the current authorization status of the Avaya CMS features and capacities.

```
Version purchased:   R16.3
                               Capability/Capacity   Authorization
                               -------------------   -------------
                                    disk mirroring   installed
                                         vectoring   authorized
                                       forecasting   authorized
                                          graphics   authorized
                             external call history   authorized
                            expert agent selection   authorized
                              external application   authorized
                      global dictionary/ACD groups   not authorized
                            Avaya CMS Supervisor    authorized
                         Avaya CMS Report Designer   authorized
             Maximum number of split/skill members   32000
                            Maximum number of ACDs   8
          Simultaneous Avaya CMS Supervisor logins   400
                Number of authorized agents (RTU)   32000
```

Note:
The system may display different authorizations depending on the current version of Avaya CMS and the packages you installed.

Using auth_set

To use the `auth_set` option to authorize Avaya CMS features and capacities:

1. Enter **cmssvc**.

   The system displays the **CMSSVC** menu.

2. Enter **2** to select `auth_set`.

   The system displays the following message:

```
Password:
```

3. Enter the appropriate password. See Configuring Avaya CMS authorizations on page 67 for more information.

   This password is available only to authorized personnel.

Using run_ids

To use the `run_ids` option to turn IDS on and off:

1. Enter **`cmssvc`**.

   The system displays the **CMSSVC** menu.

2. Enter **`3`** to select `run_ids`.
3. Perform one of the following actions:
   - To turn on IDS, enter: **`1`**
   - To turn off IDS, enter: **`2`**

Using run_cms

To use the `run_cms` option to turn the Avaya CMS software on and off:

1. Enter **`cmssvc`**.

   The system displays the **CMSSVC** menu.

2. Enter **`4`** to select `run_cms`.
3. Perform one of the following actions:
   - To turn on the Avaya CMS software, enter: **`1`**
   - To turn off the Avaya CMS software, but leave the IDS software on, enter: **`2`**
   - To turn off both the Avaya CMS software and the IDS software, enter: **`3`**

Using setup

Use the `setup` option to set up the initial Avaya CMS configuration. When the cmssvc **`setup`** command is running, any attempt to run other **`cmsadm`** or **`cmssvc`** commands will be rejected, and the system will display the error message `Please try later, setup is active`.

Do not confuse this option with the `swsetup` option, which is used to change the switch information.

⚠ **CAUTION:**
Do not run `setup` on a system that is in service or you may lose all the customer data.

Using swinfo

Use the `swinfo` option to display the switch options that are currently assigned for each ACD.

1. Enter **`cmssvc.`**

   The system displays the **CMSSVC** menu.

2. Enter **`6`** to select `swinfo`.

   The system displays a list of ACDs.

3. Select the ACD for which you want to display the switch options.

   The system displays the following information:

   - Switch name
   - Switch model (release)
   - If Vectoring is enabled
   - If Expert Agent Selection is enabled
   - If the Central Office has disconnect supervision
   - Local port
   - Remote port
   - Link transport method (TCP/IP)

Using swsetup

Use the `swsetup` option to change the switch options for each ACD. Do not confuse this option with the `setup` option, which is used for setting up Avaya CMS.

When you change switch parameters, you should also check the parameters in the `CMS System Setup: Data Storage Allocation` window. If you enable Vectoring, you need to allocate space for VDNs and vectors. Changing the switch release may change the number of measured entities allowed and also impact the storage allocation for each entity.:

1. Turn the Avaya CMS software off:

   a. Enter **`cmssvc`**.

      The system displays the **CMSSVC** menu.

   b. Enter **4** to select `run_cms`.
   c. Enter **2** to turn off the Avaya CMS software, but leave the IDS software on.

2. Enter **cmssvc.**

   The system displays the **CMSSVC** menu.

3. Enter **7** to select `swsetup`.

   The system displays a list of ACDs.

4. Select the ACD that you want to change.
5. At the prompts, provide the following information:
   - Switch name
   - Switch model (release)
   - Is Vectoring enabled on the switch (if authorized)?
   - Is Expert Agent Selection (EAS) enabled on the switch (if authorized)?
   - Does the Central Office have disconnect supervision?
   - Local port assigned to the switch (Avaya recommends that you use 1)
   - Remote port assigned to the switch (Avaya recommends that you use 1)
   - Transport method used to connect to the switch (TCP/IP)
   - Enter the host name or IP address and TCP port

   The system displays all the information. The system then asks if the switch administration is correct.

6. If the switch information is correct, enter: **y**
7. Turn on the Avaya CMS software:
   a. Enter **cmssvc**.

      The system displays the **CMSSVC** menu.

   b. Enter **4** to select `run_cms`.
   c. Enter **1** to turn on the Avaya CMS software.

Using patch_inst

Use the `patch_inst` option to install one or more Avaya CMS patches from the software disc. If you want to install all patches, use the `load_all` command.

Note:
Some patches can only be installed if Avaya CMS is off. Refer the **read me** file on the Avaya CMS software disc to determine the state of Avaya CMS before installing a patch.

1. Insert the Avaya CMS R16.3 software disc, for the specific platform type such as SPARC or x86, into the disc drive.
2. Enter **`cmssvc`**.

   The system displays the **CMSSVC** menu**.**
3. Enter **`8`** to select `patch_inst`.
4. Enter the patch number.

   The system installs the patch and displays messages similar to the following:

```
@(#) installpatch 1.0 96/04/01
cmspx-s
Generating list of files to be patched...
Creating patch archive area...
Saving a copy of existing files to be patched...
xxxx blocks
        File compression used
Installing patch packages...

Doing pkgadd of cmspx-s package:
Installation of <cmspx-s> was successful.

Patch packages installed:
        cmspx-s

Patch installation completed.
```

5. After you install all of the required patches, enter:

   `eject cdrom`

   For more details about CMS patches, see Working with Avaya CMS patches on page 198.

Using patch_rmv

Use the `patch_rmv` option to remove a single Avaya CMS patch installed on the machine.

1. Enter **`cmssvc`**.

   The system displays the `CMSSVC menu`.
2. Enter **`9`** to select `patch_rmv`.
3. Enter the patch number.

   The system removes the patch.
4. Repeat Steps 2 and 3 for each patch that you want to remove.

   For more details about CMS patches, see Working with Avaya CMS patches on page 198.

Using load_all

Use the `load_all` option to install all Avaya CMS patches from the software disc.

Note:
Some patches require the Avaya CMS software to be off. Look at the **readme** file on the CMS software disc to determine the state of CMS before attempting to install a patch.

1. Insert the Avaya CMS software disc, for the specific platform type such as SPARC or x86, into the disc drive.
2. Enter **`cmssvc`**.

   The system displays the **CMSSVC** menu.
3. Enter **`10`** to select `load_all`.
4. Enter: **`y`**

   The system installs the patches and displays messages similar to the following:

```
@(#) installpatch 1.0 <date>
cmspx-s
Generating list of files to be patched...
Creating patch archive area...
Saving a copy of existing files to be patched...
xxxx blocks
        File compression used
Installing patch packages...

Doing pkgadd of cmspx-s package:
Installation of <cmspx-s> was successful.

Patch packages installed:
        cmspx-s

Patch installation completed.
```

5. After installing all the patches, enter:

   `eject cdrom`

   For more details about Avaya CMS patches, see Working with Avaya CMS patches on page 198.

Using back_all

Use the `back_all` option to remove all Avaya CMS patches installed on the machine.

1. Enter `cmssvc`.

   The system displays the **CMSSVC** menu.

2. Enter `11` to select `back_all`.

   The system removes all the installed patches and displays a conformation message for each patch that was removed.

   For more detailed information about Avaya CMS patches, see Working with Avaya CMS patches on page 198.

The Avaya CMS backups

CMS R16.2 or later supports CMS backups to multiple backup devices. Pre R16.2 CMS systems only supported CMS backups to tape. CMS systems earlier than R16.2 only supported CMS backups to tape. Using CMS, you cannot take simultaneous backups of any type, even if multiple backup device types are administered.

Avaya CMS maintenance backups only save Avaya CMS data (administration and historical) and the Avaya CMS data for each Automatic Call Distribution (ACD). You must perform Avaya CMSADM backups to save the CMS system data, such as OS.

- After the Avaya CMS is provisioned
- After the Avaya CMS software is upgraded
- On a daily basis.

You can perform these backups within the Avaya CMS software. For more information, see *Avaya Call Management System Administration*.

Note:
If you use the Avaya CMS LAN backup feature, back up your Avaya CMS data according to *Avaya Call Management System 16 LAN Backup User Guide*. This document provides information about using the Avaya CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

CMSADM backup

The CMSADM file system backup saves all local file systems on the computer onto a backup device, including:

- Solaris system files and programs
- Avaya CMS programs

Important:
The CMSADM backup does *not* save Avaya CMS data tables. During the CMSADM backup no users, other than those logged in before the CMSADM backup was started, are allowed to log into the CMS system.

This section includes the following topic:

- When to perform a CMSADM backup on page 162

Note:
If you use the Avaya CMS LAN backup feature, back up your system data according to *Avaya Call Management System Release 16 LAN Backup User Guide*. This document provides information about using the Avaya CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

When to perform a CMSADM backup

Perform the CMSADM file system backup:

- A CMSADM backup should be performed after the CMS is provisioned to backup the Solaris system files, system programs and Avaya CMS configuration data placed on the computer by TSC provisioning personnel. These CMSADM backups can be to tape, a USB storage device or a network mount point and should also be saved and not reused or overwritten.

  Important:
  A set of default backup tapes with the factory configuration are shipped with the CMS system. These tapes must be saved and never reused in case the system needs to be reinstalled in the field.

- After the Avaya CMS system is provisioned

  This backup contains the Solaris system files and programs and Avaya CMS configuration data placed on the computer by TSC provisioning personnel. These tapes should also be saved and not reused.

  In addition, field technicians should perform an Avaya CMS full maintenance backup before they turn a new system over to the customer. For more information, see *Avaya Call Management System Release 16 Administration*.

- Before and after the Avaya CMS software is upgraded (usually performed by a field technician)
- Once a month (performed by the customer).

⚠ **Important:**
You must document the CMS systems, their OS version information and their associated Backup/Restore Device information to aid in disaster recovery of CMS.

To determine the Solaris Release and Version information, enter:

```
more /etc/release
```

Below are examples of the type of information that needs to be saved:

CMS Hostname	Solaris Release and Version
trapper1	Solaris 10 10/08 s10s_u6wos_07b SPARC
Your CMS system	

CMS Hostname	Backup/ Restore Device Type (Tape/ USB/ Network)	Backup/Restore Device Path	Backup/Restore Device Name	Description
trapper1	USB	/CMS_Backup	USB_trapper1	USB backup for trapper1
Your CMS system				

⚠ **Important:**
Unlike tape devices, USB storage devices and network mount points must be monitored to ensure they are accessible. Timetables and Backup/Restore Devices using USB storage devices and network mount points must be able to access these media sources to function properly. Remember to remount all non-tape media sources, used by CMS, after any reboot of the system.

Backing up the CMS system

This section includes the following topics:

- Backing up the CMS system to a tape

- Backing up the CMS system to a USB storage device
- Backing up the CMS system to a Network mount point

Backing up the CMS system to tape

Tape drives and cartridges

The following table lists the models of tape drives that are supported.

Tape drive	Tape cartridge	CMS computers
DAT 72	DDS compliant 170 meter 36/72-GB DAT cartridge 4 mm	Sun SPARC Enterprise T5120 Sun SPARC Enterprise T5220
LTO-4	820 meter 800 GB LTO-4 cartridge 12.65 mm	Sun SPARC Enterprise T5120 Sun SPARC Enterprise T5220 Sun Netra X4270
LTO-5	846 meter 1.5 TB LTO-5 cartridge 12.65 mm **Note**: LTO-4 cartridges can also be used in the LTO-5 drive.	Sun SPARC Enterprise T5120/T5220 Sun Netra X4270 Sun SPARC T4-1

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

Performing a CMSADM backup to tape

To perform a CMSADM backup to tape:

1. Verify that:
   - The computer is in a Solaris multi-user state (2 or 3). To check whether you are in the multi-user state, enter: `who -r`
   - You are using the correct tape for the tape drive on your system.

CAUTION:
Use a new set of backup tapes for this CMSADM file system backup. Do NOT use the original set of factory backup tapes or provisioning backup tapes. Make sure that there are enough tapes for the new backup.

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

   `cmsadm`

   The system displays the **Avaya Call Management System Administration** Menu.
4. Enter the number associated with the `backup` option.

   Depending on the configuration of your system, the system displays one of the following options:

   - If only one tape drive is available on the system, go to Step 5.
   - If more than one tape drive is available for use by the system, the system displays a list of tape devices. Enter a tape drive selection from the displayed list.

   The system displays the following message:

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

5. Press **Enter**.

   The backup process begins. If more than one tape is required, the system displays the following message:

```
End of medium on "output".
Please remove the current tape, number it, insert tape number x,
and press Enter
```

6. If the system displays the message in Step 5, insert the next tape and allow it to rewind. When it is properly positioned, press **Enter**.
7. When the backup is completed, the system displays information according to the number of tapes that are required for the backup:

- If the number of tapes required is one, go to Step 10.

  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 (Rxxxxx.x)
```

- If the number of tapes required is more than one, the system displays the following message:

```
xxxxxxx blocks
Tape Verification
Insert the first tape
Press Return to proceed :
```

8. Insert the first tape to be used in the backup and press **Enter**. Wait for the LED on the tape drive to stop blinking before you remove the tape.
9. When prompted, repeat Step 8 for any additional tapes generated by the backup process. When the final tape is verified, the program 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 (Rxxxxx.x)
```

10. Label all tapes with the:
    - Tape number
    - Date of backup
    - Current version of Avaya CMS
11. Set the tape write-protect switch to read-only and put the tapes in a safe location.

    If you have problems performing a CMSADM backup, see CMSADM backup problems on page 260.

Checking the contents of the CMSADM backup tape

The system lists the files on the backup tape so you can determine if the backup has saved the correct information or verify that a particular file has been saved.

Note:
It can take a long time to display the file names on the backup tape.

To check the contents of the CMSADM backup tape:

1. Insert the first backup tape.
2. To list the files on the tape, enter the following command on a single line:

   ```
   nohup cpio -ivct -C 10240 -I /dev/rmt/dev# -M “Insert tape %d and
     press Enter” | tee
   ```

   where ***dev#*** is the device name.

   The system displays a list of files.
3. If you are not sure of the device path, enter:

   ```
   mt -f /dev/rmt/dev# status
   ```

   where ***dev#*** is the device name.

   The device name is usually `/dev/rmt/0c`. However, the device name used depends on the drive’s SCSI ID. Possible device names are:

`/dev/rmt/0`	Indicates the first noncompressing tape drive with the lowest target address
`/dev/rmt/1`	Indicates the second noncompressing tape drive with the second lowest target address
`/dev/rmt/0c`	Indicates the first compressed-mode tape drive with the lowest target address
`/dev/rmt/1c`	Indicates the second compressed-mode tape drive with the second lowest target address

   The correct device path will show information similar to the following:

   ```
   HP DAT 72(Sun) tape drive:
      sense key(0x0)= No Additional Sense   residual= 0   retries= 0
      file no= 0   block no= 0
   ```
4. After you have seen the files you are looking for or have confirmed that data on the tape is accurate, press **Delete** to stop the display.

Backing up the CMS system to a USB storage device

This section contains the ffollowing topics:

Configuring and Connecting a USB storage device

The customer is responsible for the proper configuration of the USB storage device and connectivity to the CMS system. CMS only supports USB Removable Mass Storage devices formatted using the UFS (Solaris SPARC only) or ZFS (Solaris SPARC or Solaris x86) file systems. Solaris may detect USB storage devices formatted with other file system types but CMS only supports the file systems mentioned above. If your USB storage device is formatted with any file system type, you will need to reformat the device using UFS or preferably ZFS. The USB storage device must be formatted, Solaris will not allow an unformatted USB storage device to be mounted.

Note:

You cannot use CMS to manage the filesystem on the USB device or NFS mounts. CMS will continue to write backups to the device until all space is used up. The customer is responsible for taking care of all *file rotation* activities. In this manner, a customer with an extra large NFS area could save 20 copies of the CMSADM backup for their system, whereas a customer with a small USB stick might only want to keep 2 copies on that device.

Important:
Avaya recommends that customers with large CMS configurations such as T5220, T5120 8-core, and SPARC T4 do not use USB Storage devices for data backups. It is the responsibility of the customer to ensure that the CMS system detects the USB storage device and users can perform read and write operations to and from the USB storage device. This document provides information as a reference to aid in troubleshooting USB storage device recognition issues but you should NOT contact Avaya to resolve any issues with your USB storage devices. Instead, contact your system administrator to resolve any USB storage device issues. Ensure you can write to and read from the installed USB storage devices before performing any Maintenance or CMSADM backups.

Verifying the USB storage device is recognized by the CMS system

Output from the rmformat command provides information that may be needed to mount the USB storage device.

1. Insert the USB storage device.
2. Disable the volfs service since it can interfere with ZFS.

   `svcadm disable volfs`
3. Enter: **`rmformat`**

Note:
`rmformat` is defined as removable media format.

The output of the `rmformat` command is shown below:

```
Looking for devices...
  1.Volmgt Node: /vol/dev/aliases/cdrom0
    Logical Node: /dev/rdsk/c0t0d0s2
    Physical Node: /pci@0/pci@0/pci@l/pci@0/pci@l/pci@0/usb@0,2/
storage@2/disk@0,0
    Connected Device; TSSTcorp CD/DVDW TS-T632A 3R03
    Device Type: DVD Reader/Writer
  2.Volmgt Node: /voi/dev/aliases/rmdisk0
    Logical Node: /dev/rdsk/c6t0d0s2
    Physical Node: /pci@0/pci@0/pci@l/pci@0/pci@l/pci@0/usb@0,2/hub@4/
storage@2/dlsk@0,0
    Connected Device: Kingston DataTraveler 2.0 PMAP
    Device Type: Removable
  3.Volmgt Node: /vol/dev/aliases/rmdiskl
    Logical Node: /dev/rdsk/c7t0d0s2
    Physical Node: /pci@0/pci@0/pci@l/pci@0/pci@1/pci@0/usb@0,2/
storage@1/disk@0,0
    Connected Device: HDT72252 5DLATSO V440
    Device Type: Removable
```

Note:
On Solaris x86 systems, the l`ogical_device_path` will end with a `p0` instead of the `s2` as is shown in the example above.

The Logical Node, Connected Device and Device Type information is used to identify the USB storage devices. Connected Device identifies manufacturer and model information. Device Type identifies the type of device. USB storage devices are identified as "Removable". Locate all devices that are identified as " Removable". Use the Connected Device information to locate the specific USB storage device of interest.

Examine items 2 and 3 from the `rmformat` output above. These items are USB storage devices and are identified as Removable devices. Note that the Logical Node for item 2 is identified as `/dev/rdsk/c6t0d0s2`, which identifies the controller and slot information of the device.

4. Determine the size and available disk space of a USB storage device. Refer to the Avaya CMS Administration Guide for information on how to determine the amount of space needed for a maintenance backup of data.

Note:
Do not run this command if a backup is running since the device is already under heavy use.

Enter: **`df -kl`**

Note:
If multiple USB storage devices are installed but some devices are not displayed with the `df -kl` command, then the USB storage device is probably not formatted properly. Contact your system administrator to correctly configure the USB storage device. The information below is for reference only and should only be performed by experienced personnel.

5. Determine the file system type of a USB storage device.

   Enter: **`fstyp <logical_node_path>`**

   Example: `fstyp /dev/dsk/c3t0d0p0`

   - If the output of the **`fstyp`** command is UFS and you do not wish to change it to ZFS, continue with Step 10.
   - If the output of the **`fstyp`** command is ZFS, continue with Step 11.
   - If the output of the **`fstyp`** command is not UFS or ZFS, continue with Step 6.

6. Formatting the USB storage device as ZFS.

Note:
UFS was used on SPARC systems with CMS R16.2. The ZFS filesystem works reliably on Solaris x86 systems, so it is preferred that you format all new USB storage devices with ZFS in CMS R16.3.

CAUTION:
Formatting a USB storage device will overwrite all data on the USB storage device and all data will be lost. Be sure you are certain you want to remove all data on the USB storage device. If you do not want to remove the data on the USB storage device, replace the USB storage device with a different USB device that can be formatted, and restart this procedure from Step 3.

You must create the ZFS filesystem in the root directory. The ZFS filesystem name or the pool name that you specify in the `zpool create` command must not include any slashes (/) so it can not be a subdirectory. The ZFS filesystem name or pool name must be unique or it will write over any existing directory. Avaya recommends that you create the ZFS mount points in the root directory to prevent problems due to administrators misplacing or forgetting mount point information.

a. To change to the root directory, enter:

```
cd /
```

b. To create the ZFS filesystem on the USB storage device, enter:

```
zpool create -f -o version=22 CMS_Backup {device_path}
```

where

`device_path` is the device path, which is the `logical_node_path` with `rdsk` replaced by `dsk`.

Example:

```
zpool create -f -o version=22 CMS_Backup /dev/dsk/c3t0d0p0
```

WARNING:
No warnings are given about overwriting old data. Do not run this command unless you are sure you do not want any data from the USB stick.

The USB stick is now available at `/CMS_Backup`. You can use a different name but ensure that you are not using an existing directory name.

c. You may now re-enable volfs using:

```
svcadm enable volfs
```

d. Continue with step 11.

7. Formatting the USB storage device as UFS.

   CAUTION:
   Verify that the device path entered is listed in the `rmformat` command output for the USB drive. Failure to enter the correct device path for the USB drive could result in a system outage. Formatting a USB storage device overwrites all data on the USB storage device and all data is lost. Ensure you want to remove all data on the USB storage device. If you do not want to remove the data on the USB storage device, replace the USB storage device with a different USB device that can be formatted, and restart this procedure from Step 3.

   a. Identify the Logical Node of the device to be formatted.

      Enter: **`fdisk <logical_node_path>`**

      Example: `fdisk /dev/rdsk/c6t0d0s2`

      In the above example the Logical Node path of the USB storage device is `/dev/rdsk/c6t0d0s2`.

      The system displays messages similar to the following:

```
           Total disk size is 30515 cylinders
           Cylinder size is 16065 (512 byte) blocks

                Cylinders
Partition Status Type Start End Length %
========= =========== ========= ===== ===
   1       IFS: NTFS 0  30514  30515 100




SELECT ONE OF THE FOLLOWING:
   1. Create a partition
   2. Specify the active partition
   3. Delete a partition
   4. Change between Solaris and Solaris2 Partition IDs
   5. Exit (update disk configuration and exit)
   6. Cancel (exit without updating disk configuration)
Enter Selection:
```

b. Select the option to **Delete a partition**.

```
Specify the partition number to delete (or enter 6 to exit):
```

Enter the appropriate Partition number.

The system displays messages similar to the following:

```
Are you sure you want to delete partition X? This will make all
files and programs in this partition inaccessible (type "y" or
"n").
```

Enter: **y**

c. Repeat Step 6.b until all current partitions are deleted.

The system displays messages similar to the following:

```
Total disk size is 30515 cylinders
        Cylinder size is 16065 (512 byte) blocks

                Cylinders
Partition    Status  Type  Start End   Length   %
=========    ======  ===== =========   =====   ===




SELECT ONE OF THE FOLLOWING:
   1. Create a partition
   2. Specify the active partition
   3. Delete a partition
   4. Change between Solaris and Solaris2 Partition IDs
   5. Exit (update disk configuration and exit)
   6. Cancel (exit without updating disk configuration)
Enter Selection:
```

d. Select the option to **Create a partition**.

The system displays messages similar to the following:

```
Select the partition type to create:
1=SOLARIS2  2=UNIX        3=PCIXOS     4=Other
5=DOS12     6=DOS16       7=DOSEXT     8=DOSBIG
9=DOS16LBA  A=x86 Boot    B=Diagnostic C=FAT32
D=FAT32LBA  E=DOSEXTLBA   F=EFI        0=Exit?
```

e. Select the option for **UNIX**.

The system displays messages similar to the following:

```
Specify the percentage of disk to use for this partition
(or type "c" to specify the size in cylinders).
```

f. Partition 100% of the disk:

Enter: 100

The system displays messages similar to the following:

```
Should this become the active partition? If yes, it  will be
activated each time the computer is reset or turned on.
Please type "y" or "n".
```

Enter: **n**

The system displays messages similar to the following:

```
         Total disk size is 30515 cylinders
         Cylinder size is 16065 (512 byte) blocks

Partition   Status       Type      Start   End   Length   %
=========   ======    ============  =====   ===   ======   ===
  1                   Unix system   1     30514  30514   100



SELECT ONE OF THE FOLLOWING:
   1. Create a partition
   2. Specify the active partition
   3. Delete a partition
   4. Change between Solaris and Solaris2 Partition IDs
   5. Exit (update disk configuration and exit)
   6. Cancel (exit without updating disk configuration)
Enter Selection:
```

Select the option to "Exit (update disk configuration and exit)".

8. Create the UFS file system on the USB storage device.

   Enter: **`newfs <logical_node_path>`**

   The system displays messages similar to the following:

   ```
   newfs: construct a new file system /dev/rdsk/c7t0d0s2: (y/n)?
   ```

   Enter: **y** to continue.

   The system displays messages similar to the following:

   ```
   Warning: 142 sector(s) in last cylinder unallocated
   /dev/rdsk/c10t0d0s2:    490223474 sectors in 79789 cylinders of 48 tracks,
   128 sectors
           239366.9MB in 4987 cyl groups (16 c/g, 48.00MB/g, 5824 i/g)
   super-block backups (for fsck -F ufs -o b=#) at:
    32, 98464, 196896, 295328, 393760, 492192, 590624, 689056, 787488,
   885920,
   Initializing cylinder groups:
   ```

Note:
Formatting the disk may take a long time depending on the speed and size of the disk.

9. Verify the file system type for the USB storage device is type UFS.

   Enter: **`fstyp <logical_node_path>`**

   - If the output of the `fstyp` command is UFS, continue with Step 10.
   - If the output of the `fstyp` command is not UFS, repeat Steps 7-9. If the `fstyp` cannot be configured properly, try using a different USB storage device.

Note:
If the system displays a message that `fstyp` cannot open the device, verify that `volfs` has been disabled. Refer to Step 2.

10. Mount the USB storage device.

    a. Create the mount point if the mount point does not exist, enter:

       `mkdir /{mount_point}`

       Example: `mkdir /CMS_Backup`

    b. To mount the USB storage device, enter:

       `mount  /dev/dsk/c#t#d0s2  /{mount_point}`

       where `c#t#` is the controller and slot assignment.

       Example: `mount  /dev/dsk/c6t0d0s2  /CMS_Backup`

c. To verify the USB storage device is mounted, enter:

   `ls -l /{mount_point}`

   Example: `ls -l /CMS_Backup`

   The USB storage device directory should display a message similar to the following:

```
drwx------ 2 root root 8192 Oct 8 15:33 lost+found
```

d. Turn on volmgt by entering the following step:

   `svcadm enable volfs`

11. Verify files can be written to and read from the USB storage device by creating a file on the USB storage device and accessing the file from the USB storage device.

Note:
Read and write permissions for the backup directories just created may need to be updated so that system and data backups can be performed by any user authorized to run these backups.

Mounting a USB storage device

1. Insert the USB storage device.
2. To mount the USB storage device using ZFS, enter:

   `zpool import -a -f`

3. To display the ZFS pool name, enter:

   `zpool list`

Note:
If the USB mount point was created in the root directory, the above command displays the ZFS pool name. Avaya recommends that you create the USB mount points in the root directory to prevent problems due to administrators misplacing or forgetting mount point information.

4. To mount a USB storage device with UFS, enter:

   `svcadm disable volfs`

   `mount {mount_point}`

   Example: `mount /CMS_Backup`

Note:
The USB mount_point path must exist.

   `svcadm enable volfs`

Unmounting a USB storage device

1. To unmount the USB storage device using ZFS, enter:

   `zpool export {ZFS_pool_name}`

2. If you are not sure of the ZFS pool name, enter:

   `zpool list`

3. To unmount a USB storage device with UFS, perform the following steps to unmount the device.

   Enter: **`umount /CMS_Backup`**

Note:
USB storage devices used by timetables and backups must be mounted for them to function properly. Remember to remount all non-tape Backup/Restore Devices after any reboot of the system.

Administering a Backup/Restore Device for a USB storage device

A Backup/Restore Device must be administered before a CMSADM or Maintenance backup to a USB storage device can be performed.

Note:
The Backup/Restore Devices screen limits the length of the path name that can be entered so keep the directory names as short as possible.

1. Open the CMS main menu and select **Maintenance>Backup/Restore Devices**. The Maintenance Backup/Restore Devices screen is displayed.

   a. Enter a Device name.

   b. Enter the Path of the USB storage device.

      Example: `/CMS_Backup`

   c. Enter a Description.

   d. Select the Device Type **Other.**

   e. Select **Add.**

      If the USB storage device path entered does not exist, a message similar to the following will be displayed:

```
Path not valid for type “Other”.
Press return to continue:
```

      To resolve this issue, be sure the USB storage device is accessible and the directory path exists.

   f. To view the administered backup devices, select **List devices.**

Performing a CMSADM backup to a USB storage device

1. Verify that:
   - The computer is in a Solaris multi-user state (2 or 3). To check whether you are in the multi-user state, enter:

     `who -r`
   - The USB storage device is installed and configured.
   - To determine the size and available disk space of the USB storage device, enter:

     `df -kl`

   CAUTION:
   Ensure the USB storage device has enough space for this CMSADM system backup.
2. Log in as root.
3. Enter:

   `cmsadm`

   The system displays the `Avaya Call Management System Administration Menu.`
4. Enter the number associated with the backup option.

   Depending on the configuration of your system, the system displays the following options:

```
Choose a backup device:
  1) Tape
  2) Other
Enter choice (1-2) or q to quit:
```

5. Select the number for the **Other** option.
6. Enter the Path of the USB storage device (the path must not be located on the CMS disk).

   Example: `/CMS_Backup`
7. The CMSADM back up begins. To monitor the progress of the CMSADM backup, enter:

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

   When the backup is completed, the system displays messages similar to the following:

```
9399920 blocks
Backup Verification
9399920 blocks

Backup file is located at /home/CMS_Backup/CMSADM-r16.3ef.j-120330010438-bayliss
```

8. Avaya recommends that CMSADM backup files written to USB storage devices be saved to another location for disaster recovery.

Performing a CMS Maintenance Back Up of data to a USB storage device

1. From the CMS main menu select **Maintenance>Back Up Data.**

   The Maintenance Backup Data screen is displayed.

2. Select **List devices** to view the available backup devices.
3. Press **F5** to close the list of devices window.
4. Enter the USB storage Device name.
5. Select **Run** to perform the Maintenance Back Up of Data.

   If the Verification field is set to y a message similar to the following is displayed:

```
WARNING: Your named device "USB_rmdisk1" is not a tape storage
Device and you have requested a tape verification. If
you choose to continue, the verify request will
be ignored.
Enter yes to continue or no to cancel.
Enter y or Y for yes, n or N for no:
```

6. Select **y** to continue.
7. The Maintenance back up of data begins. You can monitor the progress of the data backup by entering:

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

   Messages similar to the following will be written to the `/cms/maint/backup/back.log` when the backup successfully completes.

```
state: 1
/cms/install/bin/compress_backup successfully finished: Monday, October
11, 2010
 10:34:24 PM MDT
error:
status: Last backup finished 10/11/2010 22:34:40.
state: 0
```

8. Avaya recommends that CMS Full Maintenance backup files written to USB storage devices be saved to another location for disaster recovery.

Checking the contents of the CMSADM backup to USB

The system lists the files on the USB storage device so you can determine if the backup has saved the correct information or verify that a particular file has been saved.

Note:
It can take a long time to display the file names on the USB storage device.

To check the contents of the CMSADM backup to a USB storage device:

1. Insert the USB storage device.
2. To list the files on the USB storage device, enter:

   ```
   ls -l  /{mount_point}
   ```

   Example: `ls -l /CMS_Backup`
3. To list the individual CMSADM files on the USB storage device, enter the following command on a single line:

   ```
   cpio -ivct -C 10240 -I /{mount_point}/<CMSADM_filename> | more
   ```

   where <`CMSADM_filename`> is the filename of the CMSADM backup file of interest.

   Example: `cpio -ivct -C 10240 -I /CMS_Backup/ CMSADM-r16.2da.d-101019110736-trapper1 | more`

   Note: The name of the CMSADM backup file identifies the following:

   Type of backup: `CMSADM`

   CMS version at the time of the backup: `r16.2da.d`

   Date of the backup: `101019 (yymmdd)`

   Unique identifier of the backup: `110736`

   CMS hostname: `trapper1`
4. After you have seen the files you are looking for or have confirmed that data on the USB storage device is accurate, press Delete to stop the display.

Backing up the CMS system to a network mount point

This section contains the following topics:

- Configuring and Connecting to a network mount point on page 180
- Administering a Backup/Restore Device for a network mount point on page 187
- Performing a CMSADM backup to a network mount point on page 188
- Performing a CMS Maintenance Back Up of data to a network mount point on page 189
- Checking the contents of the CMSADM backup to a network mount point on page 190

Configuring and Connecting to a network mount point

The customer is responsible for the proper configuration of network mount points and connectivity to the CMS system.

⚠ **Important:**
Contact your system administrator before creating any shared mount points or network mount points. It is the responsibility of the customer to determine if any security violations will be made by creating share points and allowing other systems on the network to access the share points. Creating and sharing mount points should only be performed by experienced personnel.

It is the responsibility of the customer to ensure that the CMS system detects the network mount point and users can perform read and write operations to and from the network mount point. This document provides information as a reference to aid in troubleshooting network mount point recognition issues but you should NOT contact Avaya to resolve any issues with your network mount points. Instead, contact your system administrator to resolve any network mount point issues. Be sure you can write to and read from network mount points before performing any Maintenance or CMSADM backups.

network_server_mt_pt_dir	Network server directory that will be mounted from the CMS system as an NFS mount point
CMS_fqdn	Fully qualified domain name of the CMS system

Configuring a NFS server

The customer is responsible for the proper configuration and connectivity between the NFS server and CMS system. The CMS system does not permit a CMSADM backup and a Maintenance backup to be performed simultaneously, even if multiple backup device types are administered. The following points must be kept in mind while using NFS mounted directories:

- The NFS mount point must be accessible from the CMS system.
- The NFS server must have enough disk space for the backup of data.
- The directory path used when administering an NFS Back Up Device must exist on the NFS server.

The following procedures will provide basic information about configuring a NFS server and CMS system to support NFS backups and restores:

- If the network server is Solaris, continue with Solaris 10 NFS server configuration on page 182.
- If the network server is Linux, continue with Linux NFS server configuration on page 185.

Note:
You cannot use CMS to manage the filesystem on the USB device or NFS mounts. CMS will continue to write backups to the device until all space is used up. The customer is responsible for taking care of all *file rotation* activities. In this manner, a customer with an extra large NFS area could save 20 copies of the CMSADM backup for their system, whereas a customer with a small USB stick might only want to keep 2 copies on that device.

Solaris 10 NFS server configuration

Perform the following steps on the Solaris network server.

Note:
These steps are NOT performed on the CMS system itself. They are performed on the NFS server which must be a separate, non CMS, customer provided Solaris computer.

1. To create the network_server_mt_pt_dir, enter:

   ```
   mkdir /network_server_mt_pt_dir
   ```

   Example:

   ```
   mkdir /data
   mkdir /data/cms_data
   ```

2. Set the permissions for the network_server_mt_pt_dir, enter:

   ```
   chmod 755 /network_server_mt_pt_dir
   chown nobody:nobody /network_server_mt_pt_dir
   ```

Note:
Later, if you are unable to write to the network mount point on the CMS server indicated by a "Permission denied" message on the CMS server, you must set the owner and group to `nfsnobody`. Enter:

```
chown nfsnobody:nfsnobody /network_server_mt_pt_dir
```

3. To share the Solaris network server, edit `/etc/dfs/dfstab` and add a line with the Solaris network server directory that will be shared:

   a. vi `/etc/dfs/dfstab`

   b. Append the Solaris network mount point information to the bottom of the file:

   ```
   share -F nfs -o rw=<CMS_FQDN>  /network_server_mt_pt_dir
   ```

   where <CMS_FQDN> is the FQDN of the CMS system.

   Example:

   ```
   share -F nfs -o rw=igor.dr.avaya.com  /data/cms_data
   ```

   c. Write and save the file.

4. Enable NFS network server:

   ```
   svcadm -v enable -r network/nfs/server
   ```

5. To verify the network service is online, enter:

   ```
   svcs | grep nfs
   ```

6. Restart NFS to activate the share, enter:

   ```
   svcadm restart network/nfs/server
   ```

7. To share all administered mount points, enter:

   ```
   shareall
   ```

8. To see what mount points are being shared, enter:

   ```
   share
   ```

9. To unshare a single mount point, enter:

   ```
   unshare /network_server_mt_pt_dir
   ```

10. To unshare all administered mount points, enter:

    ```
    unshareall
    ```

11. Perform the following steps on the CMS system.

network_server_mt_pt_dir	Network server directory where the CMS system will write and read backup data
NS_backup_dir	CMS directory for mounting the Network server directory

Note:
The Backup/Restore Devices screen limits the length of the path name that can be entered so keep the directory names as short as possible.

12. To create the network mount point directory, enter:

    ```
    mkdir /NS_backup_dir
    ```

    Example: `mkdir /igor_cms_backups`

13. To add the Solaris network mount point to `/etc/vfstab`, enter:

    a. **vi** **`/etc/vfstab`**

⚠ **WARNING:**
Be very careful when making changes to the `/etc/vfstab` file. You must not change existing entries in this file or the system can fail to boot properly.

b. Append the Solaris network mount point information to the bottom of the file

```
network_server:/network_server_mt_pt_dir - /NS_backup_dir nfs -
  yes rw,bg,soft,intr,retry=10,vers=3
```

Example:

```
igor:/data/cms_data - /igor_cms_backups nfs - yes
rw,bg,soft,intr,retry=10,vers=3
```

c. Write and save the file.

14. To mount the network server mount point directory, enter:

```
mount /NS_backup_dir
```

15. To change to the network server mount point directory, enter:

```
cd /NS_backup_dir
```

16. To list the contents of the network server mount point directory, enter:

```
ls -l
```

Note:
The contents of this directory should be the same as that of the directory contents of the actual network server mount point directory.

17. To determine the size and available disk space of the network server mount point directory, enter:

```
df -k
```

Note:
There should be adequate space to backup the data. The data compression rate is very high on most systems. Refer to *Avaya CMS Administration* for information on how to determine the amount of space needed for a maintenance backup of data.

18. To unmount a network server mount point directory, enter:

```
umount /NS_backup_dir
```

Note:
Network server mount points used by timetables and backups must be mounted for them to function properly. Remember to remount all non-tape Backup/Restore devices after unmounting.

19. Continue with Administering a Backup/Restore Device for a network mount point on page 187.

Linux NFS server configuration

Perform the following steps on the Linux network server.

Note:
These steps are not performed on the CMS system itself. They are performed on the NFS server which must be a separate, non-CMS, customer provided Linux computer.

1. To create the `network_server_mt_pt_dir`, enter:

   `mkdir /network_server_mt_pt_dir`

   Example:

   ```
   mkdir /data
   mkdir /data/cms_data
   ```

2. Set the permissions for the `network_server_mt_pt_dir`, enter:

   `chmod 755 /network_server_mt_pt_dir`

   `chown nobody:nobody /network_server_mt_pt_dir`

Note:
Later, if you are unable to write to the network mount point on the CMS server indicated by a "Permission denied" message on the CMS server, you must set the owner and group to `nfsnobody`. Enter:

`chown nfsnobody:nfsnobody /network_server_mt_pt_dir`

3. To allow other systems to access the `network_server_mt_pt_dir`:

   a. vi `/etc/exports`

   b. Append the Linux network mount point information to the bottom of the file:

   `/network_server_mt_pt_dir <CMS_FQDN>(rw,sync)`

   Example: `/data/cms_data igor.dr.avaya.com(rw,sync)`

   c. Write and save the file.

4. To configure NFS and portmap to start on reboot:

   a. Log in as **`root`**.

   b. At the command line enter: **`ntsysv`**

   c. A GUI interface is started. Scroll through the list provided and verify that the nfs and portmap options are selected. These two options should be marked with an x.

   d. Enter TAB to highlight OK.

   e. Click on OK.

5. Starting the NFS service:

Note:
When the `/etc/exports` file is changed, it is necessary to stop and start the NFS server.

a. If the NFS service is not running, enter:

```
/etc/init.d/nfs start
```

b. If the NFS service is running, enter:

```
/etc/init.d/nfs restart
```

6. To verify the network service is running, enter:

```
service nfs status
```

7. Perform the following steps on the CMS system.

network_server_mt_pt_dir	Network server directory where the CMS system will write and read backup data
NS_backup_dir	CMS directory for mounting the Network server directory

Note:
The Backup/Restore Devices screen limits the length of the path name that can be entered so keep the directory names as short as possible.

8. To create the network mount point directory, enter:

```
cd /
mkdir /NS_backup_dir
```

Example: `mkdir /igor_cms_backups`

9. To add the Linux network mount point to `/etc/vfstab`, enter:

```
a. vi /etc/vfstab
```

⚠ **WARNING:**
Be very careful when making changes to the `/etc/vfstab` file. You must not change existing entries in this file or the system can fail to boot properly.

b. Append the network mount point information to the bottom of the file:

```
network_server:/network_server_mt_pt_dir - /NS_backup_dir nfs -
  yes rw,bg,soft,intr,retry=10,vers=3
```

Example:

```
igor:/data/cms_data - /igor_cms_backups nfs - yes
rw,bg,soft,intr,retry=10,vers=3
```

c. Write and save the file.

10. To mount the network server mount point directory, enter:

    ```
    mount /NS_backup_dir
    ```

11. To change to the network server mount point directory, enter:

    ```
    cd /NS_backup_dir
    ```

12. To list the contents of the network server mount point directory, enter:

    ```
    ls -l
    ```

    Note:
    The contents of this directory should be the same as that of the directory contents of the actual network server mount point directory.

13. To determine the size and available disk space of the network server mount point directory, enter:

    ```
    df -k
    ```

    Note:
    There should be adequate space to backup the data. The data compression rate is very high on most systems. Refer to *Avaya CMS Administration* for information on how to determine the amount of space needed for a maintenance backup of data.

14. To unmount a network server mount point directory, enter:

    ```
    umount /NS_backup_dir
    ```

    Note:
    Network server mount points used by timetables and backups must be mounted for them to function properly. Remember to remount all non-tape Backup/Restore devices after unmounting.

Administering a Backup/Restore Device for a network mount point

The user must administer a Backup/Restore device before a CMSADM or Maintenance backup to a network mount point can be performed.

Note:
The Backup/Restore Devices screen limits the length of the path name that can be entered so keep the directory names as short as possible.

1. Open the CMS main menu and select **Maintenance>Backup/Restore Devices**. The Maintenance Backup/Restore Devices screen will be displayed.

    a. Enter a Device name.

    b. Enter the Path of the network mount point.

    ```
    /NS_backup_dir/CMS_hostname
    ```

    Example: `/igor_cms_backups/trapper1`

Note:
The `/NS_backup_dir/CMS_hostname` directory must exist on the network server.

c. Enter a Description.

d. Select the Device Type **Other**.

e. Select **Add.**

If the directory does not exist on the network server a message similar to the following will be displayed:

```
Path not valid for type "Other".
Press return to continue:
```

To resolve this issue be sure the network server is mounted and the directory exists on the network server.

f. To view the administered backup devices, select **List devices.**

Performing a CMSADM backup to a network mount point

1. Verify that:
   - "The computer is in a Solaris multi-user state (2 or 3). To check whether you are in the multi-user state, enter:

     `who -r`
   - The network directory is installed and configured.
   - To determine the size and available disk space of the network mount point, enter:

     `df -k`

   CAUTION:
   Ensure the network mount point has enough space for this CMSADM system backup.
2. Log in as root.
3. Enter:

   `cmsadm`

   The system displays the **Avaya Call Management System Administration** Menu.

4. Enter the number associated with the backup option.

   Depending on the configuration of your system, the system displays the following options:

   ```
   Choose a backup device:
     1) Tape
     2) Other
   Enter choice (1-2) or q to quit:
   ```

5. Enter the number associated with the backup option.
6. Select the number for the **Other** option.
7. Enter the path of the mounted CMS (the path must not be located on the CMS disk).

   `/NS_backup_dir/CMS_hostname`

   Example: `/igor_cms_backups/trapper1`

8. The CMSADM back up begins. To monitor the progress of the CMSADM backup, enter:

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

   When the backup is completed, the system displays messages similar to the following:

   ```
   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 (Rxxxxx.x)
   ```

9. Avaya recommends that you save CMSADM backup files written to network directories to another location for disaster recovery.

Performing a CMS Maintenance Back Up of data to a network mount point

1. From the CMS main menu select **Maintenance>Back Up Data**

   The **Maintenance Backup Data** screen is displayed.

2. Select **List devices** to view the available backup devices.
3. Press **F5** to close the list of devices window.
4. Enter the network directory name.

5. Select **Run** to perform the Maintenance Back Up of Data.

   If the Verification field is set to **y** the system displays the following message:

```
WARNING: Your named device "/CMS_backup_dir/CMS_hostname" is not a tape
storage
Device and you have requested a tape verification. If
you choose to continue, the verify request will
be ignored.
Enter yes to continue or no to cancel.
Enter y or Y for yes, n or N for no:
```

6. Select **y** to continue.
7. The Maintenance back up of data begins. You can monitor the progress of the data backup by entering:

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

   Messages similar to the following will be written to the `/cms/maint/backup/back.log` when the backup successfully completes.

```
error:
status: Last backup finished 10/08/2010 02:21:41.
state: 0
/cms/install/bin/compress_backup -c /CMS_backup_dir/CMS_hostname
started:
Tuesday, October 12, 2010  8:30:53 AM MDT
check space for CMS backup
Available space: 98823688KB
```

Checking the contents of the CMSADM backup to a network mount point

The system lists the files on the network mount point so you can determine if the backup has saved the correct information or verify that a particular file has been saved.

Note:
It can take a long time to display the file names on a network mount point.

To check the contents of the CMSADM backup to a network mount point:

1. To list the files on the network mount point, enter:

   `ls -l  /NS_backup_dir/CMS_hostname`

2. To list the the individual CMSADM files on the network mount point, enter the following command on a single line:

   ```
   cpio -ivct -C 10240 -I /NS_backup_dir/CMS_hostname/
     <CMSADM_filename> | more
   ```

   where `<CMSADM_filename>` is the filename of the CMSADM backup file of interest.

   > Example: `cpio -ivct -C 10240 -I /igor_cms_backups/trapper1/ CMSADM-r16.2da.d-101019110736-trapper1 | more`
   >
   > where the name of the CMSADM backup file identifies the following:
   >
   > Type of backup: `CMSADM`
   >
   > CMS version at the time of the backup: `r16.2da.d`
   >
   > Date of the backup: `101019 (yymmdd)`
   >
   > Unique identifier of the backup: `110736`
   >
   > CMS hostname: `trapper1`

   The system displays a list of files.

3. After you have seen the files you are looking for or have confirmed that data on the network mount point is accurate, press **Delete** to stop the display.

Changing the system date and time

This section describes how to change the UNIX system date and time. For example, a change due to daylight savings time.

This section includes the following topics:

- Checking the Solaris system date and time on page 191
- Setting the system date and time on page 192
- Setting the system country and time zones on page 192

Checking the Solaris system date and time

To verify that the system time is correct:

1. Enter:

   ```
   date
   ```

2. If the system time is correct there is no need to proceed further with this procedure. If the system time is not correct, continue with Setting the system date and time on page 192.

Setting the system date and time

Do the following steps to change the Solaris system time:

1. Turn off the Avaya CMS software.
2. Log in as **root**.
3. Enter the root password.
4. Set the time and date by entering:

   ```
   date mmddHHMM[yyyy]
   ```

   Example:

   - *mm* (month): Enter the month (numeric). Range: 1-12 (1=January, 2=February, and so on).
   - *dd* (day): Enter the day of the month. Range: 1-31
   - *HH* (hour): Enter the hour of day, military time. Range: 00-23.
   - *MM* (minute): Enter the minute of the hour. Range: 00-59.
   - *[yyyy]* (year): Entering the year is optional. Enter the year, with all four digits (for example, 2000).
5. Continue with Setting the system country and time zones on page 192.
6. Turn on the Avaya CMS software.

Setting the system country and time zones

To set the country and time zones:

1. Log in as root and enter the root password.
2. Enter:

   ```
   vi /etc/default/init
   ```

3. Edit the **/etc/default/init** file and set the TZ variable to equal the appropriate value in the **/usr/share/lib/zoneinfo** directory.

   For example:

   You would modify the line with TZ=US/Mountain.

```
# @(#)init.dfl 1.2 92/11/26
#
# This file is /etc/default/init. /etc/TIMEZONE is a symlink to this file.
# This file looks like a shell script, but it is not. To maintain
# compatibility with old versions of /etc/TIMEZONE, some shell constructs
# (i.e., export commands) are allowed in this file, but are ignored.
#
# Lines of this file should be of the form VAR=value, where VAR is one of
# TZ, LANG, or any of the LC_* environment variables.
#
TZ=US/Mountain
```

4. Save and quit the file by pressing **Esc** and entering:

   :wq!

5. Reboot the machine by entering:

   /usr/sbin/shutdown -i6 -g0 -y

Working with Solaris patches

When you upgrade your Avaya CMS software, or administer a new Avaya CMS installation, you may need to:

- Verify what Solaris patches are currently installed
- Install a Solaris patch
- Remove one or more Solaris patches.

This section includes the following topics:

- Installing Solaris patches on page 194
- Checking installed Solaris patches on page 197
- Removing a Solaris patch on page 197

Installing Solaris patches

To install the Solaris patches:

1. Insert the Avaya Call Management System software disc, for the specific platform type such as SPARC or x86, into the disc drive.
2. Enter:

   `cd /`
3. Enter:

   `cmssvc`

   The system displays the **Avaya Call Management System Services** Menu (`CMSSVC Menu`).
4. Enter the number associated with the `run_cms` option.
5. Enter the number associated with the `Turn off CMS but leave IDS running` option.

   The system returns to the command prompt.
6. Set the IDS environment by entering:

   `. /opt/informix/bin/setenv`
7. Enter:

   `onmode -yuk`

   Ignore any error messages.

CAUTION:
The Avaya CMS software must be off in order to install the Solaris patches.

8. Enter:

   `/cdrom/cdrom0/spatches_conf`

   The system displays a message similar to the following:

```
Warning: you must close all applications before running this script
..................
..................
..................
Solaris patches have been spooled to your machine.  The patches will
be installed after rebooting.  During the installation of patches
your
server will not be available.

The estimated time to install all patches is: 15 minutes

Ready to install Patches. Please leave the CD in the drive.
You will need to reboot the server for patches to install.

Do you want to reboot now?  [y,n,?]
```

Note:
The system will display the approximate amount of time needed to install the Solaris patches.

9. Choose one of the following steps:

   - To install the Solaris patches:

     a. Enter: **`y`**

        The system boots into single user mode and installs the Solaris patches.

Note:
If there are no Solaris patches to install the system displays the following message.

```
There are no Solaris patches to install
```

b. Choose one of the following steps:

   – If Solaris patches were installed, go to Step 10.

   – If no Solaris patches were installed, log into the system as **root**. Then go to Step 12.

- To cancel installation of the Solaris patches, enter: **n**

  The system displays the following message:

```
Terminating at user's request.
You will need to run spatches_conf again to install Operating System
patches.
```

CAUTION:
If you cancel installation of the Solaris patches, you will have to install them before upgrading the Avaya CMS software.

10. Log into the system as **root**.
11. Verify that all of the Solaris patches have been installed by entering:

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

    The system displays the following message in the log:

```
All patches installed successfully.
```

Note:
If the installation procedure fails for any of the patches, the following message is displayed:

```
Installation failed for one or more Solaris patches.

- 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.
Patch installation completed: Fri Jan 18 13:28:19 MST 2002
```

If the message shown above is displayed, continue with this procedure and the remaining Avaya CMS base load upgrade procedures. When the upgrade is complete, notify your Avaya CMS support organization as instructed.

12. Enter:

    `eject cdrom`

Checking installed Solaris patches

To check the Solaris patches:

1. Enter:

   `showrev -p`

   The system displays the following message:

```
Patch: 105084-02  Obsoletes:   Packages: SUNWx25a.2 9.1,PATCH=02,
SUNWx25b.2 9.1,PATCH=02
Patch: 105256-01  Obsoletes:   Packages: SUNWcsu
Patch: 103582-14  Obsoletes:   Packages: SUNWcsu, SUNWcsr
Patch: 103594-10  Obsoletes:   Packages: SUNWcsu
   .
   .
   .
```

2. Check the list to verify that all the Solaris patches you need are installed.

Removing a Solaris patch

To remove a Solaris patch:

CAUTION:
Remove a Solaris patch only when instructed by the TSC or by a release letter.

1. Enter:

   `patchrm` ***`patch-id`***

   The ***`patch-id`*** is identified by the TSC or in the release letter.

   The system removes the patch, and displays the following message:

```
@(#) backoutpatch 3.5 93/08/11
Doing pkgrm of SUNWcsr.8 package:

Removal of <SUNWcsr.8> was successful.
Restoring previous version of files
    .
    .
    .
XXXX blocks
Making the package database consistent with restored files:
backoutpatch finished.
#
```

2. Enter:

   ```
   /usr/sbin/shutdown -y -g0 -i6
   ```

   The system reboots.

Working with Avaya CMS patches

This section provides procedures for maintaining patches for Avaya CMS on a Sun platform.

This section includes the following topics:

- Avaya CMS patch requirements on page 198
- Listing installed Avaya CMS patches on page 199
- Listing Avaya CMS patches on the software disc on page 199
- Installing Avaya CMS patches on page 199
- Removing Avaya CMS patches on page 201

Avaya CMS patch requirements

The three occasions when you may have to install Avaya CMS patches are:

- During a factory installation
- Immediately after upgrading the Avaya CMS software
- In the field on an existing system to correct a problem with the original software.

Loading patches after an upgrade:

If you are loading patches immediately after upgrading your system, it is best to turn off the Avaya CMS software until you have the patches installed. The patches have different prerequisites for installation. Some require that the Avaya CMS software be turned off, others require that data collection be turned off, and still others require the Avaya CMS software to be in single-user mode. To be absolutely safe, and to help the upgrade proceed as quickly as possible, turn off the Avaya CMS software.

Loading patches as a bug fix:

If you are loading patches as part of a factory installation or on an existing system in the field without upgrading your base load, you can install the patches without turning the Avaya CMS software off. The system will display a message if you need to do anything special to accomplish the load.

The Avaya CMS patch **readme** file lists the run-level requirements for each patch.

Note:
The `auth_set` tool must have been run sometime in the past before you can install patches. Call the National Customer Care Center or your product distributor to have authorizations installed.

Installation of all available patches is recommended. If you believe that you should not be installing a particular patch, call the National Customer Care Center or consult with your product distributor before deciding to omit installation of a patch.

Listing installed Avaya CMS patches

To list Avaya CMS patches currently installed on your system:

1. Log in as **root**.
2. Enter the following command:

   ```
   /cms/toolsbin/listcmspatches
   ```

   The system displays a list of Avaya CMS patches that are installed on the system.

Listing Avaya CMS patches on the software disc

To list Avaya CMS patches that are on the software disc and available to be installed:

1. Log in as **root**.
2. Insert the Avaya CMS software disc, for the specific platform type such as SPARC or x86, into the disc drive.
3. Enter:

   ```
   cmssvc
   ```

   The system displays the **CMSSVC** menu.
4. Enter the number associated with the `patch_inst` option.

   The system lists the names of the patches on the software disc.
5. Enter: **`q`**

Installing Avaya CMS patches

To install the Avaya CMS patches:

1. Log in as **root** and insert the Avaya CMS software disc, for the specific platform type such as SPARC or x86, into the disc drive.

2. Enter:

   `cd /`

3. Enter:

   `cmssvc`

   The system displays the **CMSSVC** menu.

4. Perform one of the following actions:

   - To load all of the patches, enter the number associated with the `load_all` option.
   - To load one patch at a time, enter the number associated with the `patch_inst` option.

   The system lists the patches on the software disc and asks if you really want to install the patches.

   If no patches are found on the software disc continue to next step.

   The system displays the following message:

```
No CMS patches found on the CD.
Please check the CD and try again.
```

   Perform one of the following actions if patches are found on the software disc:

   - If you want to load all of the patches, enter: **`y`**
   - If you want to load only one patch, enter the patch number.

   The system installs the patch or patches. As it does so, it displays messages similar to the following for each patch installed:

```
@(#) installpatch 1.0 96/04/01
cmspx-s
Generating list of files to be patched...
Creating patch archive area...
Saving a copy of existing files to be patched...
xxxx blocks
        File compression used
Installing patch packages...

Doing pkgadd of cmspx-s package:
Installation of <cmspx-s> was successful.

Patch packages installed:
        cmspx-s

Patch installation completed.
```

   - If no patches are found on the software disc, go to Step 5.

5. Enter:

   `eject cdrom`

Removing Avaya CMS patches

To remove Avaya CMS patches:

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

   `cmssvc`

   The system displays the **CMSSVC** menu.
3. Choose one of the following actions:
   - If you want to remove all of the Avaya CMS patches, enter the number associated with the `back_all` option.

     The system lists the patches installed on the system and asks for verification of the removal.
   - If you want to remove a single patch:
     a. Enter the number associated with the `patch_rmv` option.

        The system lists the patches that are installed on the system and prompts you to select a patch.

     b. Type the name of the patch that you want to remove exactly as it is displayed in the list, and press **Enter**.

        The system asks you to verify the removal.
4. Enter: **`y`**

   The system displays messages similar to the following example for each patch that is removed:

```
@(#) backout patch 1.0 96/08/02

Removing patch package for cmspx-s:
. . . ..

Making package database consistent with restored files:
Patch x has been backed out.
```

Adding and removing users from password aging

If a password is aged, the user will be forced to change their password after a specified amount of time. All Avaya CMS and UNIX users are effected by the `passwd_age` option in the CMSADM menu unless they are added to the password aging exclude file. For more information about using the `passwd_age` option in the CMSADM menu, see Using passwd_age on page 148.

CAUTION:
Do *not* manually edit password files. Modify the password files using the procedures in this section. Incorrectly editing password files can result in the system having to be rebuilt back to factory standards.

This section includes the following topics:

- Determining if a password is aged on page 202
- Excluding users from password aging on page 203
- Removing users from the password aging exclude file on page 204
- Aging specific passwords at different rates on page 204

Determining if a password is aged

To determine if a password is being aged:

1. Enter:

   `passwd -s` ***`user_name`***

   where ***`user_name`*** is the name of the user.

   The system will display one of the following messages:

   - If a new user has not created their password, the system displays the following message:

```
user1 NP
```

Note:
The user's password will not age unless it is created.

   - If the user's password is not aged, the system displays the following message:

```
user1 PS
```

- If the user's password is being aged, the system displays the following message:

```
user1 PS    05/20/02    0  14  7
```

Note:
The message includes the user name, the password status, the date the password was last changed, the minimum numbers of days required between password changes, the maximum number of days the password is valid, and the number of days the user will be warned before the password expires.

- If the user's password is locked, the system displays the following message:

```
user1 LK
```

Excluding users from password aging

It is recommended that you exclude specific users before turning password aging on in order to avoid additional password administration. You may need to exclude specific Avaya CMS or UNIX users from password aging. Some custom applications use Avaya CMS logins.

To exclude a specific password from being aged:

1. Log into the system as **root**.
2. Determine the password status of the user by entering:

   passwd -s *user_name*

   where ***user_name*** is the name of the user. For more information, see Determining if a password is aged on page 202.
3. Enter:

   cd /cms/db
4. Enter:

   vi age_pw_exclude
5. Add the user name you want to exclude from password aging.
6. Save and close the file by pressing **Esc**. Then enter:

   :wq!
7. If password aging was previously in effect for the user, enter:

   passwd -x -1 *user_name*

   where ***user_name*** is the name of the user, and

   where 1 is the number one.

Removing users from the password aging exclude file

Users that have been added to the exclude file will not age.You can remove a specific user from the password aging exclude file. Users that are removed from the exclude file will age normally.

To remove a specific user from the exclude file:

1. Log into the system as **root**.
2. Determine the password status of the user by entering:

   ```
   passwd -s user_name
   ```

   where *user_name* is the name of the user. For more information, see Determining if a password is aged on page 202.
3. Enter:

   ```
   cd /cms/db
   ```
4. Enter:

   ```
   vi age_pw_exclude
   ```
5. Remove the user name for the password you want to age.
6. Save and close the file by pressing **Esc**. Then enter:

   ```
   :wq!
   ```
7. Enter:

   ```
   passwd -x maxdays -w 7 user_name
   ```

   where *maxdays* is the number of days before the password expires, and

   where *user_name* is the name of the user you want to age.

Aging specific passwords at different rates

The password aging option in the `CMSADM menu` globally effects users. Individual users can have their passwords aged at different rates.

To age a specific user:

1. Log into the system as **root**.
2. Determine the password status of the user by entering:

   ```
   passwd -s user_name
   ```

   where *user_name* is the name of the user. For more information, see Determining if a password is aged on page 202.

3. Enter:

   ```
   passwd -x maxdays -w warning user_name
   ```

   where ***maxdays*** is the number of days before the password expires, and

   where ***warning*** is the number of days a password aging warning is displayed before the password expires, and

   where ***user_name*** is the name of the user you want to age.

Note:
The system will not display a password aging warning for users who only access Avaya CMS through Supervisor. Supervisor users will be prompted to enter a new password when their current password expires. Only users who access Avaya CMS through the command line will receive a warning message before their password expires.

Maintaining the chkDisks crontab

The chkDisks crontab runs each night and checks to see whether any potential or actual drive problems have been logged. For example, loss of the primary boot drive. The results of the search are mailed to the root user.

This section includes the following topics:

- Verifying chkDisks on page 205
- Changing the chkDisks run time on page 206
- Canceling chkDisks on page 206

Verifying chkDisks

To verify that `cron` is running:

1. Enter at the `#` prompt:

   ```
   crontab -l
   ```

2. Check the listing to see that there is an entry for chkDisks.

Changing the chkDisks run time

The line tells the system to run chkDisks every day at 15 minutes past hour zero (12:15 AM). You can change that schedule by changing the first five fields as necessary. The fields, in order of appearance, are: minute, hour, day of the month, month of the year, and day of the week. An asterisk means “all legal values.” The /olds/chkDisks line in the **cron** file is generally in the following format:

```
15 0 * * * /olds/chkDisks > /dev/null 2>&1
```

For more information, see the manual (man) page for the crontab command.

Canceling chkDisks

To stop cron from running:

1. Enter at the `#` prompt:

   `crontab -e`

2. With the file loaded in the editor, comment out the entry for chkDisks and write and quit the file.

Report Query Status

CMS R16.2 or later have added two types of report query logs. These logs track the queries made by historical reports and they show the queries that have completed and the queries that are currently being run. This information can be used to determine who is running what reports and if those report queries are affecting system performance.

Information about query logs

- Types of report query logs:
  - qlog: a log where entries are made upon query completion
  - idbm log: a log showing the query that is currently running
- These logs are always in operation implying that they do not need to be turned off/on
- Comparison between the report query logs
  - qlog has more detail, but is only updated after the report query has completed

  - idbm log shows currently running queries and is updated at completion of the query to add completion status

- Uses of report query logs
  - qlog can show past report execution to determine who ran queries and how long the queries took
  - idbm log can be used to determine what queries are running currently. This can be used to determine if a particular query is taking a long time and thus negatively impacting system performance.
  - Log information in either logs cannot be used to kill a particular report; it is debug information only
- qlog features
  - Entries are made upon query/report completion
  - Applies to historical report queries only
  - Log entries have information about start time, user, run time, completion status, task ID and query text
  - qlogs are stored in directory `/cms/db/log` as `qlog, qlog.01, qlog.02`, etc.
  - CMS administers the size and number of qlog files in the file `/cms/db/LogAdmin/qlog` on the server
  - Example entry:

```
Mon Sep 13 00:35:50 2010 USER=dsb123    TIME=00:00 STATUS=0     TASK=13018
QUERY=select vdn, starttime, intrvl, acdcalls, acdtime, abncalls,
busycalls,disccalls,incalls,othercalls from hvdn where row_date = 40432
and acd = 1  order by vdn, starttime
```

- idbm log features
  - The system makes entries for currently running queries.
  - Applies to historical report queries only.
  - IDBM stands for Informix Database Manager. These are the processes that interface with the historical database.
  - Log entries contain information about start time, user and query text.
  - The idbm logs are kept in the server in directory `/cms/db/log` as idbm.'process ID'. For example: `idbm.17, idbm.1001, idbm.13027`, etc.
  - Example entry:

```
Tue Sep 14 16:32:33 2010 dsb123 select value, item_name from synonyms
where item_type='split' and acd_no=1
```

  - If no query is running in that idbm process, the log will show the last query run along with its status.

- Example status entry:

```
Tue Sep 14 16:32:33 2010 STATUS=0
```

Recovering an Avaya CMS system

This section provides the procedures for recovering data on a Call Management System (CMS) that has non-functioning hardware or software corruption. Personnel at the Technical Service Center (TSC) will need assistance from an on-site technician or the site's CMS administrator in order to perform most of the procedures in this chapter.

This section includes the following topics:

Using the nohup command

When executing commands that take a long time to complete, such as `cpio` commands, use the `nohup` command to ensure that the command completes without interruption if the data line disconnects.

An example of the `nohup` command is:

```
nohup cpio -icmudf -C 10240 -I <backup_media_path> "cms" | tee
```

where `backup_media_path` depends on the media type.

Examples:

Tape	`/dev/rmt/dev#`
USB storage device	`/CMS_Backup/<CMSADM_filename>`
Network mount point	`/NS_backup_dir/CMS_hostname/<CMSADM_filename>`

When system reboots are required, verify that your terminal type is set correctly after the reboot.

Performing a CMS maintenance restore

This section describes how you can restore CMS data from a CMS maintenance backup. You can restore data from a full maintenance backup as well as from full/incremental maintenance backups.

⚠ **CAUTION:**
If you are performing this procedure because of a disk replacement or crash, Recovering a mirrored system after disk failure on page 216 before performing this procedure.

This section includes the following topics:

- Data restore requirements on page 210
- Restoring data from a full maintenance backup on page 211
- Restoring data from a full and incremental maintenance backup on page 212
- Restoring data using a binary backup on page 214
- Using tapeless migration on page 216

Data restore requirements

Before you perform a CMS maintenance restore, you must meet the following requirements depending on the type of data you wish to restore:

Data to be restored	System requirements
Historical and non-CMS	● The CMS software can be in a multiuser state ● Data collection can be on
Local system administration	● The CMS software must be in the single-user state ● Data collection must be turned off
ACD-specific administration	● The CMS software must be in the single-user state ● Data collection can be on
CMS system administration	● The CMS software must be in the single-user state ● Data collection can be on

Restoring data from a full maintenance backup

⚠ **CAUTION:**
Perform this procedure when only the full Avaya CMS maintenance backups are available. If an incremental maintenance backup is also available, see Restoring data from a full and incremental maintenance backup on page 212.

1. Load, install, or mount the most recent full maintenance backup media.

   Note:
   At this point the system will not contain any customer defined Backup/Restore Devices for USB storage devices or network mount points. If the backup media is on a USB storage device or network mount point you will need to create a Backup/Restore Device, using the CMS menu options **Maintenance | Backup/Restore Devices**, before the data can be restored. If the backup media is on a USB storage device refer to the section Administering a Backup/Restore Device for a USB storage device on page 177. If the backup media is on a network mount point refer to the section Administering a Backup/Restore Device for a network mount point on page 187.

2. From one of the windows at a console, log in to the system by using a CMS administrator login ID, for example, `su - cms`. Enter the correct password if prompted.
3. Enter `cms.`

   A series of prompts about system status may appear before the system displays the CMS main menu.
4. Enter the correct terminal type.
   - If the CMS version on the backup media is the same CMS version installed on the system then the data can be restored, continue with Step 5.
   - If the CMS version on the backup media is the not the same CMS version installed on the system then the data needs to be migrated, continue with Step 7.
5. Select the **Maintenance** option.
6. Select the **Restore Data** option.

   In the `Restore from last backup (y/n)` field, enter: `n`

   Continue with Step 9.
7. Select the `System Setup` option.
8. Select the **R3 Migrate Data** option.

   Continue with Step 9.
9. Enter the Device name that you want to restore/migrate data from. This can be the name of the tape device, the NFS mount point or the USB storage device. You can get the device names by pressing **Enter**, selecting `List devices` and pressing **Enter** again.

10. For the remaining options, do not make any changes.
11. Press **Enter**, select **Run** and press **Enter** again.

    Note:
    To execute a Restore/Migrate operation, CMS has to be in single user mode and data collection for the switch has to be turned off.

12. The system restores/migrates the system administration data, ACD-specific data, historical data, and non-CMS data.

    Note:
    If the restore/migrate action fails, select **Maintenance>Error Log Report** to analyze the cause of failure.

13. Go to the Free Space Allocation window that is located in the CMS System Setup subsystem and verify that no adjustments need to be made. For more information about Free Space Allocation, see *Avaya Call Management System Administration*.

Restoring data from a full and incremental maintenance backup

CAUTION:
Perform this procedure only if both full and incremental Avaya CMS maintenance backups are available. If only a full maintenance backup is available, see Restoring data from a full maintenance backup on page 211.

1. Load, install, or mount the most recent full maintenance backup media.
2. From one of the windows at a console, log in to the system by using a CMS administrator login ID, for example **su - cms**. Enter the correct password if prompted.
3. Enter `cms`.

   A series of prompts about system status may appear before the system displays the CMS main menu.
4. Enter the correct terminal type.
5. Depending on the type of data to be restored, it may not be necessary to perform Steps a or b. See the table in Data restore requirements on page 210 to determine which steps to perform.
   a. To change the CMS software to single user mode:
      1. Select **System Setup - CMS State**.

         The system displays the **CMS State** window.
      2. Enter an **x** in the `Single-user mode` field and press **Enter** twice.
      3. Press **F5** to return to the main menu.

   b. Turn off data collection:

   1. Select **System Setup - Data Collection**.

      The system displays the **Data Collection** window.

   2. Enter the name of the ACD.
   3. Use **Tab** to move the `Off` field and enter: **`x`**
   4. Press **Enter**, select `Modify`, and press **Enter** again.
   5. Repeat Steps 1 through 4 for each ACD.
   6. Press **F5**.

      The system displays the CMS main menu.

6. Select **Maintenance - Restore Data**.
7. In the **Restore Data** window, select the following options:

Item	Values specified or selected

`Device name`	`Tape Device name`
	`USB storage device name`
	`Network Device name`

`Restore from last backup?`	`n`
`Restore historical data from`	(leave blank)
`ACDs to restore`	`All ACDs`

`Data to restore`	`Local System Administration data`
	`ACD-specific administration data`
	`Historical data`
	`Non-CMS data`

8. Press **Enter**, select `Run`, and press **Enter** again.
9. When the full maintenance restore is finished:
   a. Remove the full backup media and insert the most current incremental backup media.
   b. Repeat Steps 7 and 8 as needed.
   c. Continue with Step 10.
10. After the incremental restore is finished, press **F5**.

    The system displays the CMS main menu.

11. Depending on the type of data to be restored, it may not be necessary to perform Steps a or b. See the table in Data restore requirements on page 210 to determine which steps to perform.

    a. Turn data collection on:

       1. Select **System Setup - Data Collection**.

          The system displays the Data Collection window.

       2. Enter the name of the ACD.

       3. Use the **Tab** key to move to the `On` field and enter: **`x`**

       4. Press **Enter**, select `Modify`, and press **Enter** again.

       5. Repeat Steps 1 through 4 for each ACD.

       6. Press **F5**.

          The system displays the CMS main menu.

    b. Take the Avaya CMS software out of single user mode:

       1. Select **System Setup - CMS State**.

          The **CMS State** window displays.

       2. Enter an **`x`** in the `Multi-user mode` field and press **Enter** twice.

       3. Press **F5**.

          The system displays the Avaya CMS main menu.

12. Select **Logout** and press **Enter**.

13. Go to the **Free Space Allocation** window that is located in the `CMS System Setup` subsystem and verify that no adjustments need to be made.

    For more information about Free Space Allocation, see *Avaya Call Management System Release 16 Administration*.

Restoring data using a binary backup

You can restore the data either from a tape or from a network device.

Restore database using a binary backup from tape

1. Log in to the CMS server as root.

2. Do one of the following:

   - If a CMSADM restore was performed to recover the system due to system failures, disk crashes, or power outages, continue with Step 3.
   - If a CMSADM restore was not performed to recover the system, continue with Step 6.

3. Insert the CMSADM backup tape into the tape drive.
4. Change to the root directory:

   ```
   cd /
   ```

5. To restore custom reports, enter:

   ```
   cpio -imudv -C 10240 -I /dev/rmt/0 "cms/db/gem/c_custom/*" "cms/
     db/gem/h_custom/*" "cms/db/gem/r_custom/*"
   ```

6. Insert the binary backup tape into the tape drive.
7. To restore the database enter:

   ```
   /cms/install/bin/db_restore <tape_device>
   ```

   If a <tape_device> is not entered, the default device will be **/dev/rmt/0c**.

Restore database using a binary backup from a mount point

To restore a binary backup from a USB storage device or a network mount point, perform the following steps:

1. Log in to the CMS server as root
2. Do one of the following:
   - If you performed a CMSADM restore to recover the system due to system failures, disk crashes, or power outages, continue with Step 3.
   - If you performed a CMSADM restore to recover the system, continue with Step 6.
3. Mount the backup device containing the CMSADM backup.
4. Change to the root directory:

   ```
   cd /
   ```

5. To restore custom reports, which are backed up as part of the CMSADM backup, enter the following command on a single line:

   ```
   cpio -imudv -C 10240 -I {mount_point/CMSADM_filename} "cms/db/gem/
     c_custom/*" "cms/db/gem/h_custom/*" "cms/db/gem/r_custom/*"
   ```

   where `backup_media_path` is dependent on the media type.

   Example of `backup_media_paths`:

USB storage device	`/CMS_Backup/<CMSADM_filename>`
Network mount point	`/NS_backup_dir/<CMSADM_filename>`

6. If the mount point to the binary backup file does not exist, remount the mount point and verify it is accessible.

Note:
If a mount point does not exist perform one of the following steps to create the mount point:

- If the binary backup file is on a USB storage device refer to Configuring and Connecting a USB storage device on page 168.
- If the binary backup file is on a network server refer to Configuring and Connecting to a network mount point on page 180.

7. Execute the restore script:

```
/cms/install/bin/db_restore /<mount_point/<binary_backup_filename>
```

Using tapeless migration

Tapeless migration is necessary when upgrading from a system that has a tape drive to a new CMS R16.3 system that does not. In this case, the RTM tool, which is available from downloads on the support site, is used to copy the CMS maintenance backup tape on the existing system to a file on the new system. Once this file is created, you can migrate data from that file. The use of the RTM tool is only performed once and when the migration is completed, the customer should perform backups using one of the supported tapeless backup options for the new system. For more on tape and non-tape device compatibility, see section "Tape Compatibility" in *Avaya CMS R16.3 Platform Upgrade and Data Migration*.

Recovering a mirrored system after disk failure

This section contains procedures for the recovery of a mirrored system after disk drive failure.

⚠ **Important:**
The system will need to be rebuilt to factory standards and any data will need to be restored if both disks in a matched pair fail. If this condition is met, see Performing a CMSADM restore of a system on page 222.

This section includes the following topics:

- Prerequisites on page 217
- Recovering a system after a single disk fails on page 217
- Recovering a system after a pair of mirrored disks fail on page 221

Prerequisites

Before you recover a mirrored system, perform the following tasks:

- Verify that the alternate boot device is set up.
- Search the output for Failed or Degraded device(s).
- Identify the faulty disk or disks. See Determining which disks have failed on page 217 for more information.
- The system must boot off of a functioning boot disk.

Recovering a system after a single disk fails

Use this procedure to recover a system after a single disk failure. The T5120 and T5220 disks are hot-swappable.

1. Determine which disk should be replaced.

   See Determining which disks have failed on page 217.
2. Attach an ESD wrist strap to the metal chassis of the computer and to your wrist.
3. Remove the faulty disk and replace it with a new disk.

   The new disk will automatically synchronize.
4. Monitor the progress of the disk rebuilding by entering:

   ```
   /olds/olds  -synch-stat
   ```

Determining which disks have failed

Determine if you have the AAC or MRSAS RAID adapter in your system.

1. Verify the RAID adapter you have by entering the following:

   a. To determine that you have the AAC style RAID adapter, enter:

      ```
      grep aac /etc/path_to_inst
      ```

      This command should return the following if you have the AAC style RAID adapter:

      ```
      "/pci@0/pci@0/pci@9/scsi@0" 0 "aac"
      ```

      Otherwise, it will return the prompt only.

b. To determine that you have the MRSAS style RAID adapter, enter:

   `grep mr_sas /etc/path_to_inst`

   This command should return the following if you have the LSI style RAID adapter:

   ```
   "/pci@0/pci@0/pci@9/LSI,mrsas@0" 0 "mr_sas"
   ```

   Otherwise, it will return the prompt only.

2. If you have the AAC style RAID adapter, enter:

   `/opt/StorMan/arcconf getconfig 1 PD | egrep 'State|Device'`

   The following is an example of the command on a T5220:

```
Physical Device information
      Device #0
         Device is a Hard drive
         State                              : Online
         Reported Channel,Device            : 0,0
      Device #1
         Device is a Hard drive
         State                              : Online
         Reported Channel,Device            : 0,1
      Device #2
         Device is a Hard drive
         State                              : Online
         Reported Channel,Device            : 0,2
      Device #3
         Device is a Hard drive
         State                              : Failed
         Reported Channel,Device            : 0,3
      Device #4
         Device is a Hard drive
         State                              : Online
         Reported Channel,Device            : 0,4
      Device #5
         Device is a Hard drive
         State                              : Online
         Reported Channel,Device            : 0,5
      Device #6
         Device is an Enclosure services device
         Reported Channel,Device            : 2,0
      Device #7
         Device is an Enclosure services device
         Reported Channel,Device            : 2,1
```

Note that the Device #3 is in a Failed State. The yellow light should be on for the drive in slot 3. That is the slot with the bad disk.

You may also see the State "Degraded". This could possibly be a disk that is causing problems also. If no other disk is exhibiting "Failed" and the remove (blue) light is on for the disk, it may need replacing.

3. If you have the MRSAS style RAID adapter, enter:

   /opt/MegaRAID/CLI/MegaCli -pdlist -a0 | grep Firmware

   The following is an example of the command on a T5120 8-core:

   ```
   Firmware state: Online, Spun Up
   Firmware state: Online, Spun Up
   Firmware state: Online, Spun Up
   Firmware state: Online, Spun Up
   Firmware state: Online, Spun Up
   Firmware state: Online, Spun Up
   ```

4. Check that the proper number of responses are returned. There should be one line for each disk in the system. T5120 4-core systems should have 4 disks, T5120 8-core, T5220, and T4-1 systems should have 6 disks. Also make sure all are in the "Online, Spun Up" state. If all disks are seen and in the proper state, all disks are good and you can continue. If you see less than the expected number of disks, enter:

   /opt/MegaRAID/CLI/MegaCli -pdgetmissing -a0

   The following is an example output from a T5120 8-core with 300GB disks:

   ```
   Adapter 0 - Missing Physical Drives

   No.     Array          Row     Size Expected
   0       1              0         285148 MB
   Exit Code: 0x0
   ```

   This shows that disk 0 of Array1-Row1 is missing. This means that the disk in slot 2 of the system is missing (failed).

5. If there are no missing disks, but the state is not proper for all disks, enter:

   /opt/MegaRAID/CLI/MegaCli -pdinfo -physdrv[252:0] -a0 |pg

   /opt/MegaRAID/CLI/MegaCli -pdinfo -physdrv[252:1] -a0 |pg

   Continue running the above command for all the disks in the system, each time checking the "Firmware state:" for the problem disk(s). The output will look similar to the following for each disk:

```
Enclosure Device ID: 252
Slot Number: 4
Device Id: 25
Sequence Number: 7
Media Error Count: 0
Other Error Count: 0
Predictive Failure Count: 0
Last Predictive Failure Event Seq Number: 0
PD Type: SAS
Raw Size: 279.396 GB [0x22ecb25c Sectors]
Non Coerced Size: 278.896 GB [0x22dcb25c Sectors]
Coerced Size: 278.464 GB [0x22cee000 Sectors]
Firmware state: Offline                                      *
SAS Address(0): 0x5000cca00ad6e8b1
SAS Address(1): 0x0
Connected Port Number: 2(path0)
Inquiry Data: HITACHI H103030SCSUN300GA2A81040GU5YVE
FDE Capable: Not Capable
FDE Enable: Disable
Secured: Unsecured
Locked: Unlocked
Needs EKM Attention: No
Foreign State: None
Device Speed: 6.0Gb/s
Link Speed: 6.0Gb/s
Media Type: Hard Disk Device
Drive:  Not Certified



Exit Code: 0x00
```

   This example shows that the disk at [252:4] is Offline (see the line marked with *). This corresponds to slot 4 of the T5120 8-core, or T5220, or T4-1 system. The T5120 4-core has the same basic mapping, but will not have a disk slot 4, so this example will not apply to that system.

Recovering a system after a pair of mirrored disks fail

Use this procedure to recover a system after a pair of mirrored disks fail. Refer to the table below to determine if a pair of mirrored disks have failed. The T5120, T5220 and T4-1 disks are hot-swappable.

Sun Enterprise T5120 4-core mirrored disk pairs

Primary disk	Mirrored disk
slot 0	slot 1
slot 2	slot 3

Sun Enterprise T5220, T5120 8-core and T4-1 mirrored disk pairs

Primary disk	Mirrored disk
slot 0	slot 1
slot 2	slot 3
slot 4	slot 5

Sun Netra X4270 mirrored disk pairs

Primary disk	Mirrored disk
Slot 0	Slot 1

The mirrored pairs are shown by the inclusion within a Paranthesised group, for example (slot 0, slot 1).

Determine which disks should be replaced. For more information on determining which disks should be replaced, see Determining which disks have failed on page 217

If a mirror pair of disks have failed on either the T5120, T5220, or T4-1 platforms then the system has to be completely restored. Continue with Performing a CMSADM restore or Performing a LAN restore.

An example of a mirror pair disk failure on a T5120 or T4-1 would be that disks in slot 0 and slot 1 fail. Since disks in slot 0 and slot 1 are a pair of mirrored disks then a complete system restore is needed, you would continue with Performing a CMSADM restore or Performing a LAN restore. If disks in slot 0 and slot 2 fail then each disk is considered a single disk failure and can be replaced using the process defined under Recovering a system after a single disk failure.

An example of a mirror pair disk failure on a T5220 or T4-1 would be that disks in slot 4 and slot 5 display failure messages. Since disks in slot 4 and slot 5 are a pair of mirrored disks then a complete system restore is needed. If disks in slot 0, slot 2 and slot 5 fail then each disk is considered a single disk failure and can be replaced using the process defined under Recovering a system after a single disk failure.

Performing a CMSADM restore of a system

This section describes how to restore an entire system. You must re-enable the system to boot. Then restore the system software from the CMSADM backup tape. You will have to restore the system if a mirror pair of disks fail.

This section includes the following topics:

- Prerequisites on page 222
- Restoring a system with a restore script on page 222

Prerequisites

Before you begin restoring the system, perform the following tasks:

- Obtain the CMSADM file system backup tapes.
- Obtain the most recent maintenance backup tapes.
- Replace any defective hardware.

Restoring a system with a restore script

This section provides the procedure to restore a system with a restore script.

If the CMSADM backup file is on a USB storage device or a network mount point you will need additional information before proceeding with the restore of the CMS system. In the section *When to perform a CMSADM backup*, Avaya recommended that you keep a log of the CMS systems and their associated Backup/Restore Device information to aid in the recovery of a CMS system. Locate this information to use in this procedure. If a log of this information is not available you need to have the following information to proceed with recovering the CMS system:

- If the CMSADM restore is being performed from a USB storage device:
  - Logical Node name of the USB storage device for T5120/T5220/T4-1 systems if formatted using UFS.

  - CMS backup directory name

- If the CMSADM restore is being performed from a network mount point:

  Note:
  If the network server is not in DNS you will need the network server ip address.

  - Network server hostname
  - Network server mount point directory
  - Network server backup directory name

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

1. Perform one of the following actions:
   - If the system is powered off, continue with Step 3.
   - If the system is running, enter the following command to prepare the system for a restore:

     `/usr/sbin/shutdown -i5 -y -g0`

2. The system will display the following message (x86 platform only):

```
Press any key to reboot.
```

   Press any key then manually power off the system.

3. Replace any defective disks.

   Note:
   For more information about installing hard drives, see the appropriate *hardware installation, maintenance, and troubleshooting* guide for your platform.

4. Remove/disconnect any USB storage devices.
   - If the system is a x86 platform, continue with Step 11.
   - If the system is a T5120/T5220/T4-1 platform, continue with Step 5.

5. As the console shows that the system is booting up, press **Stop+A**.

   The system displays the `ok` prompt.

6. Enter the following commands at the `ok` prompt:

```
ok> setenv auto-boot? False
ok> reset-all
```

7. The system will reset and come back to the ok prompt. Now run the following command at the ok prompt:

```
ok> show-disks
```

Look for

`/pci@0/pci@0/pci@9/LSI,mrsas@0/disk`

for T5120/T5220 servers, or

`/pci@400/pci@2/pci@0/pci@c/LSI,mrsas@0/disk`

for T4-1 servers.

If this value is found in the list, then you have the MRSAS style RAID adapter in your system. If not, then you have the AAC style RAID adapter. Make note of the RAID adapter style and continue. There will be prompts specific to each adapter below.

- If you have the MRSAS style RAID adapter, continue with Step 8.
- If you have the AAC style RAID adapter, continue with Step 9.

8. Perform the following actions for the MRSAS style RAID adapter:

a. Enter:

```
ok> nvalias disk /pci@0/pci@0/pci@9/LSI,mrsas@0/disk
```

for T5120/T5220 servers, or

```
ok> nvalias disk /pci@400/pci@2/pci@0/pci@c/LSI,mrsas@0/disk
```

for T4-1 servers.

b. Insert the Solaris 10 SPARC software disc into the disc drive, continue with Step 10.

9. Perform the following actions for the AAC style RAID adapter:

a. Enter:

```
ok> nvalias disk /pci@0/pci@0/pci@9/scsi@0/disk@0
```

b. Press **Enter** if prompted to accept current configuration.

c. Insert the Solaris Sun StorageTek™ RAID SPARC Configuration disc into the disc drive, continue with Step 10.

10. Enter:

`boot cdrom -rsw`

The system boots from the disc, continue with Step 12.

11. Perform the following actions for the x86 platform:

    a. Power on the system.

    b. As the system boots, insert the Solaris 10 x86 software disc into the disc drive. Verify the Solaris 10 DVD is pulled into the disc drive.

    c. Select the "**Solaris**" option.

    d. Select the "**Single user shell**" option.

    Note:
    If the system displays a message about wanting to mount Solaris 10, answer no.

    e. Continue with Step 12.

12. Enter the following commands:

    ```
    stty erase Backspace
    ```

    ```
    ksh -o vi
    ```

    The system will display Backspace as ^H. On some systems Backspace will not work. If this is the case, substitute "^H" for Backspace.

13. Enter:

    ```
    pwd
    ```

    The system displays the following message:

    ```
    /tmp/root
    ```

    If the system does not display `/tmp/root`, enter:

    ```
    cd /tmp/root
    ```

    The system provides the following options for accessing the CMSADM backup media:

    - If the CMSADM backup is on tape, continue with step 14.
    - If the CMSADM backup is on a USB device formatted with ZFS, continue with step 15.
    - If the CMSADM backup is on a USB storage device formatted with UFS, continue with step 16.
    - If the CMSADM backup is on a network mount point, continue with step 18.

14. To access the CMSADM backup from tape.

    a. Insert the CMSADM backup into the tape drive.

    b. Enter the following command on a single line:

    ```
    cpio -icmudv -C 10240 -I /dev/rmt/dev# "cms/install/bin/
      restore"
    ```

    where ***dev#*** is replaced with the tape device name.

    c. Continue with step 19.

15. To access the CMSADM backup from a USB storage device formatted with ZFS:
    a. Insert the CMSADM backup USB storage device.
    b. Import the ZFS formatted USB device using the following commands:

```
mount -o remount,rw /
```

```
zpool import -a -f
```

Note:
The zpool import command may generate an SMF initialization error message when the system is booted to the Solaris DVD. Ignore this message.

The ZFS pool device is imported to the same pool name and mount point that was used to originally create it. You can verify the ZFS device was imported properly and check the pool name by entering the following command:

```
zpool list
```

Note:
To unmount a ZFS type USB storage device, enter:

```
   zpool export {ZFS_pool_name}
```

The output will look something like this:

NAME	SIZE	ALLOC	FREE	CAP	HEALTH	ALTROOT
CMS_Backup	59.5G	70.5K	59.5G	0%	ONLINE	-

where `CMS_Backup` is the name of the ZFS pool and also the name of the directory where the pool is mounted (`/CMS_Backup`). *ONLINE* is the status of the pool. If not *ONLINE*, contact your Avaya Services representative.

Enter:

```
ls -al /{pool name}
```

to ensure that files are located on the device as expected.

    c. Continue with Step 4.

16. To access the CMSADM backup from a USB storage device formatted with UFS:

⚠ **Important:**
Always mount the USB storage device on `/a`, the `/mnt` directory is used by the restore script. The USB storage device must be inserted, configured and accessible on the CMS system. Refer to Configuring and Connecting a USB storage device on page 168 for information on how to mount a USB storage device.

    a. Insert the CMSADM backup USB storage device.
    b. Mount the USB storage device using the following steps:

1. Enter: **`ls -l /dev/dsk`**

Important:
Do not mount any USB storage device on c1t0 which is reserved for RAID10. If any storage device is mounted on c1t0, be sure all USB storage devices have been removed and reboot the system.

2. Make a note of the controller number and slot number for the USB storage device, such as `c1t5`.
3. Mount the USB storage device on `/a`.

- If the USB storage device file system type is UFS, enter:

  ```
  mount /dev/dsk/c#t#d0s2 /a
  ```

- If the USB storage device file system type is ZFS, enter:

  ```
  mount /dev/dsk/c#t#d0p2 /a
  ```

  where `c#t#` is replaced with the USB controller number and slot number.

4. Enter: **`ls -l /{mountpoint}`**

   where `mountpoint` is the ZFS pool name, or *a* for UFS devices.

17. Make a note of the CMSADM backup filename of interest.

    a. Enter the following command on a single line:

    ```
    cpio -icmudv -C 10240 -I /{mountpoint}/<CMSADM_filename> "cms/
      install/bin/restore"
    ```

    where `CMSADM_filename` is the CMSADM system backup file of interest. The CMSADM filename must be entered exactly like the path on the media device.

    Example: `cpio -icmudv -C 10240 -I /CMS_Backup/CMSADM-r16.3ed.b-101019110736-trapper1 "cms/install/bin/restore"`

    where the name of the CMSADM backup file identifies the following:

    Type of backup: `CMSADM`

    CMS version at the time of the backup: r16.3ed.b

    Date of the backup: `101019 (yymmdd)`

    Unique identifier of the backup: `110736`

    CMS hostname: `trapper1`

    b. Continue with Step 19.

18. To access the CMSADM backup from a network mount point, mount the CMSADM backup network server:

    a. Enter: **`ifconfig network_interface0 unplumb`**

b. Enter: **ifconfig network_interface0 plumb**

c. Enter the following command on a single line:

   ifconfig network_interface0 inet CMS_ip netmask CMS_netmask broadcast +

   where network_interface0 is e1000g0 for T5120/T5220 systems and igb0 for x86 and T4-1 systems, CMS_ip is the ip address of the CMS system and CMS_netmask is the netmask of the network for the CMS system.

d. Enter: **ifconfig network_interface0 up**

e. Enter: **ifconfig -a**

   The system displays the following messages. Search for network_interface0 and verify the information is correct.

```
network_interface0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 2
        inet xxx.xxx.xxx.xxx netmask ffffff00 broadcast xxx.xxx.xxx.xxx
        ether xx:xx:xx:xx:xx:xx
```

f. Enter: **route add default route_ip**

   where route_ip is the ip address the network router for the CMS system.

g. Enter: **ping route_ip**

   Verify the network router for the CMS system responds.

h. Enter: **ping nfs_server**

   Verify the network server responds.

i. Enter: **mount -F nfs -o vers=3 network_server:/network_server_mt_pt_dir /a**

   Example: mount -F nfs -o vers=3 igor:/data/cms_data /a

Note:
Always mount the network mount point on /a, the directory /mnt is used by the restore script. If the network mount point is not found the cmsadm restore will fail.

j. Enter: **ls -l /a**

   Verify the contents of the network server mount point are displayed.

k. Enter the following command on a single line:

```
cpio -icmudv -C 10240 -I /a/<CMSADM_filename> "cms/install/bin/
  restore"
```

where `CMSADM_filename` is the CMSADM system backup file of interest. The CMSADM filename must be entered exactly like the path on the media device.

Example: `cpio -icmudv -C 10240 -I /a/ CMSADM-r16.2da.d-101019110736-trapper1 "cms/install/bin/ restore"`

where the name of the CMSADM backup file identifies the following:

Type of backup: `CMSADM`

CMS version at the time of the backup: `r16.2da.d`

Date of the backup: `101019 (yymmdd)`

Unique identifier of the backup: `110736`

CMS hostname: `trapper1`

l. Continue with Step 19.

19. The system retrieves the file and displays the following message within a couple of minutes:

```
cms/install/bin/restore
```

Important:
The restore script should be one of the first files on the backup media device. If the system does not display `cms/install/bin/restore` within a couple of minutes, the restore script is not on the media device. Press Ctrl+C.

Contact the National Customer Care Center, or consult with your product distributor or representative about obtaining the script.

Note:
The "`cms/install/bin/restore`" message might be displayed a second time.

20. Press Ctrl+C.

The system stops searching the CMSADM backup media device.

Note:
If you do not press Ctrl+C, the system will continue to search the entire backup media device. This search could take several hours to complete.

21. Verify that the restore script has the correct permissions by entering:

    ```
    chmod +x cms/install/bin/restore
    ```

    The system sets the correct permissions to execute the script. If the permissions for the script are not correct, the restore will fail.

22. Restore the system from the media device:

    CAUTION:
    The CMSADM backup does not preserve mount point directories. If the default backup device is a USB mount point then the restore process may fail during CMS Setup if the mount point path does not exist. If this occurs, create the mount point path and rerun CMS setup from a flatfile. Look for the default backup device path in the `/cms/install/cms_install/cms.install` file for the mount point path that needs to be created. Refer to the section Using the flat file on page 100 for instructions on how to run CMS setup from a flatfile."

    - If the backup data is on tape, continue with Step 23 on page 230.
    - If the backup data is on a USB storage device, continue with Step 24 on page 230.
    - If the backup data is on a network mount point, continue with Step 25 on page 231.

23. Restoring the system from a tape:

    a. Enter:

    ```
    cms/install/bin/restore /dev/rmt/dev#
    ```

    where ***dev#*** is replaced with the tape device name.

    b. Continue with Step 26.

24. Restoring the system from a USB storage device:

    a. Enter:

    ```
    cms/install/bin/restore /{mountpoint}/CMSADM_filename
    ```

    Example: **`cms/install/bin/restore /CMS_Backup/ CMSADM-r16.2da.d-101019110736-trapper1`**

    The system displays the following messages:

```
Attempting to set System timezone. This can take up to 60 seconds. Please
wait....
.........
.........
.........
Starting to restore. This process can take a long time.
Please wait......
```

The system will halt before building the devices directory so the USB storage device can be removed. The system displays the following messages:

```
******* Important !!*******

This looks to be a restore from a removable USB

storage device. Please remove ALL removable storage

devices, then type y to continue:
```

b. Enter: **`y`** and then press Enter.

   The system will automatically reboot after all the files on the media device have been transferred.

c. Continue with Step 28.

25. Restoring the system from a network mount point:

    a. Enter:

       `cms/install/bin/restore /a/CMSADM_filename`

       Example: `cms/install/bin/restore /a/CMSADM-r16.2da.d-101019110736-trapper1`

    b. Continue with Step 26.

26. The system displays the following messages:

```
Attempting to set System timezone. This can take up to
60 seconds. Please wait...
...................
...................
...................
Starting to restore. This process can take a long time.
Please wait...
```

- If the system is a SPARC platform, continue with Step 27.

- If the system is a x86 platform, the following message will be displayed:

```
*****  IMPORTANT  *****

Please manually eject the CD/DVD or select a different boot device after
reboot to avoid repeating the restore process.

Please enter y to continue:
```

   a. Remove the DVD from the disc drive.

   b. Enter `y` and then press **Enter**.

27. The system restores the files on the backup media. The system will automatically reboot after all the files on the media device have been transferred.

    Note:
    If a problem occurs during the restore process, the system will display prompts indicating a problem. Follow the instructions displayed by the system.

28. Log in to the system as root.

    Important:
    The system may reboot several times during the restore process. The reboots can occur at random intervals throughout the restore process. You may have to repeat this step several times.

29. After the system reboots, you can monitor the progress of the restore by entering:

    ```
    tail -f /cms/install/logdir/restore/restorecms.log
    ```

    Note:
    In order to monitor the restore progress, you must enter this command each time the system reboots.

    When the restore process is complete, the system displays the following message at the end of `restorecms.log`:

    ```
    CMS Restore Completed Successfully
    ```

30. Enter:

    ```
    ps -ef | egrep S99
    ```

31. Choose one of the following steps:

    - If a S99restorecms process is not running, go to Step 32.
    - If a S99restorecms process is running, enter the following commands:

    ```
    pkill -9 tee
    ```

    ```
    pkill -9 S99restorecms
    ```

32. Verify that the IDS software is on.
33. Turn on CMS, enter:

    `cmssvc`

    The system displays the **CMSSVC menu**.
34. Enter the number associated with the `run_cms` option.
35. Enter the number associated with the `turn on` CMS option.
36. Verify the Free Space Allocation and restore the Avaya CMS data. See Performing a CMS maintenance restore on page 210 for more information.
37. If the system has the AOM or Visual Vectors Server software installed, verify that the software is on.

Restoring a system without a CMSADM or system backup

If a CMSADM backup or system backup is not available, the system must be reinstalled with all software back to the original factory configuration.

To restore a system without a CMSADM backup or system backup:

1. Re-install the entire operating system according to Installing the Solaris operating system on page 19.
2. Configure the entire operating system according to Configuring the Solaris operating system on page 49.
3. Re-install Avaya CMS and supporting software according to Installing Avaya CMS and supporting software on page 61.
4. Restore any available Avaya CMS data from the most recent Avaya CMS maintenance backup.
5. Contact the Avaya Professional Services Organization (PSO) for any previously installed customization.

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

   `pkginfo -x cms`

   If CMS is installed, the system displays the following:

```
cms  Avaya(TM) Call Management System 64-bit
      (sparc) r17fb.e
```

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

   `/cdrom/cdrom0/cmssolasg.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.

Restoring specific files from the CMSADM backup tape

Sometimes only specific files on a system become corrupted. Use this procedure if only specific files need to be restored from a CMSADM backup tape.

Note:
If you use the Avaya CMS LAN backup feature, see *Avaya Call Management System Release 16 LAN Backup User Guide*. This document provides information about using the Avaya CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

To restore specific files from a CMSADM backup:

1. Enter:

   ```
   cd /
   ```

2. Enter the following command on a single line at the command prompt:

   - If the CMSADM backup is on tape, continue with step a.
   - If the CMSADM backup is on a USB storage device, continue with step b.
   - If the CMSADM backup is on a network mount point, continue with step c.

   a. Enter:

   ```
   cpio -icmudv -C 10240 -I /dev/rmt/dev# -M "Please remove the
     current tape, insert tape number %d,and press ENTER"
     "full_path_name"
   ```

   where **`dev#`** is replaced with the device name and **`full_path_name`** is replaced with the path of the files to be restored.

   Example:

   ```
   cpio -icmudv -C 10240 -I /dev/rmt/0 -M "Please remove the
     current tape, insert tape number %d,and press ENTER" "dev/dsk"
   ```

b. Enter:

```
cpio -icmudv -C 10240 -I /{mount_point}/<CMSADM_filename>
  "full_path_name"
```

where **`mount_point`** is the directory on the USB storage device containing the CMSADM backup file, **`CMSADM_filename`** is replaced with the CMSADM backup filename and **`full_path_name`** is replaced with the path of the files to be restored.

Example:

```
cpio -icmudv -C 10240 -I /CMS_Backup/
  CMSADM-r16.2da.d-101019110736-trapper1 "dev/dsk"
```

c. Enter:

```
cpio -icmudv -C 10240 -I /NS_backup_dir/<CMSADM_filename>
  "full_path_name"
```

where **`/NS_backup_dir`** is the network mount point path containing the CMSADM backup file, **`CMSADM_filename`** is replaced with the CMSADM backup filename and **`full_path_name`** is replaced with the path of the files to be restored.

Example:

```
cpio -icmudv -C 10240 -I /igor_cms_backups/
  CMSADM-r16.2da.d-101019110736-trapper1 "dev/dsk"
```

Troubleshooting

This section provides solutions for common software or hardware problems. Use these procedures to troubleshoot the Avaya Call Management System (CMS) software.

This section includes the following topics:

Note:

When executing commands that take a long time to complete (such as `cpio` commands), use the `nohup` command to ensure that the command will complete without interruption if the data line disconnects. An example of the `nohup` command is shown below:

```
nohup  cpio  -icmudf  -C  10240 -I <backup_media_path> “cms” |
  tee
```

When system reboots are required, verify that your terminal type is set correctly after the reboot.

Determining your Avaya CMS version

To determine the version of Avaya CMS installed on your system:

1. Enter:

   ```
   pkginfo  -x cms
   ```

   The system displays the Avaya CMS version.

Unable to read DVD

Sometimes the volfs service can be turned off by a root user or the OS, and needs to be re-enabled.

To check if the volfs service is running, enter:

```
svcs volfs
```

The output looks like :

```
STATE              STIME            FMRI
disabled           9:02:19
svc:/system/filesystem/volfs:default
```

If the service does not show "online" for STATE, run the following command to enable the service:

```
svcadm enable volfs
```

If the service was already in the "online" state, enter:

```
svcadm disable volfs
```

followed by

```
svcadm enable volfs
```

Run **svcs volfs** command again to verify the service is now "online". Retry reading your DVD. If the DVD is still not readable, contact your Avaya Services team.

Recognizing new hardware devices

Use this procedure if externally powered devices, such as disk drives and tape drives, are not recognized during a Solaris installation. This problem might occur if:

- The devices are not connected to power
- The devices are not turned on
- If you add a new port board to the computer as part of an upgrade or addition

If you discover that a hardware device is not being recognized, you must either reboot from the software disc and reinstall Solaris, or do the following (these procedures apply to T5120/T5220/T4-1 only):

1. Reboot the system by entering:

   ```
   init 0
   setenv auto-boot? False
   reset-all
   probe-scsi-all
   ```

2. Force the system to recognize the new components by entering:

   ```
   boot -r
   ```

   The system reboots.

3. Log in as **root**.

Troubleshooting password aging

This section provides options to help solve password aging problems.

This section includes the following topics:

- Tracking changes to password aging on page 240
- Passwords of excluded users age on page 240

Tracking changes to password aging

The admin log keeps a record of any administrative changes made to password aging. The system updates the admin log when the aging interval is changed or if password aging is turned on or off. The admin log can be found at **/cms/install/logdir/admin.log**

Passwords of excluded users age

If a user was added to the password aging exclude list and their password is continuing to age or has begun to age:

1. Log into the system as **root**.
2. Enter:

   ```
   passwd -x -1 user_name
   ```

   where ***`user_name`*** is the name of the user, and

   where `1` is the number one.

Avaya CMS error logs

The administrative data for each error log file contains specific information about itself, including defaults, administration information, a description of the contents, and general information about how to interpret the contents of the logs. The log provides:

- Default location

  The file name of the primary file where log information can be found if no administrative changes have been made.

- Default maximum file size

  The approximate size of each of the log files (primary and historical) that will be saved if no administrative changes have been made.

- Default number of older files retained

  The number of historical files that are kept, in addition to the primary file, if no administrative changes have been made.

- Administration file

  If the log is controlled by the general purpose file wrapping technique, the location of the file where administrative changes can be made affecting the location of the log file, the size of the logs, and/or the number of historical log files.

- Starting/stopping

  Describes the conditions necessary for the log to be running, including any appropriate commands.

- Writing process

  Indicates all processes that write to the log.

- Intended audience

  Customer (for log information that is useful to the customer, easy to read, and documented) or services (for log information that is intended to aid troubleshooting). Almost all error logs are used exclusively by services personnel.

- First implemented in load

  Indicates the first load when the log is available. The system uses an internal load numbering (such as 3.1z).

Checking installed software packages

Use this procedure to check for previously installed software packages. The rules for specifying package names are as follows:

- You can omit the ***pkgname*** variable from the command. The command then lists the name, description, and version number of every software package installed on the system.
- If you list only one package name, the command lists the name, description, and version number of only that software package.
- You can list several package names separated by spaces. The command then lists the name, description, and version number of every software package you name.

To check what software packages are installed on your system:

1. From the root prompt, enter:

   ```
   pkginfo -x pkgname
   ```

   where ***pkgname*** is the name of the software package you are checking for.

Listing pkgchk errors

The `pkgchk -n cms` command lists some common error messages that do not indicate an actual problem. The error messages in the following table can be ignored.

Location	Error message	Occurs
/cms/install/logdir/admin.log	group name <root> expected <cms> actual	After the installation and before setup.
/usr/lib/cms/pbxtrcflags	pathname does not exist	After the installation and before setup.
/cms/env/cms_mon/State_tbl	group name <bin> expected <other>actual	After the setup and before running the Avaya CMS software.
/cms/install/logdir/admin.log	group name <root> expected <cms>actual	After the setup and before running the Avaya CMS software.
/**usr/lib/cms/pbxtrcflags**	pathname does not exist	After the setup and before running the Avaya CMS software.
/cms/env/cms_mon/State_tbl	group name <bin> expected <cms> actual	After running the Avaya CMS software.
/cms/install/logdir/admin.log	group name <root> expected <cms> actual	After running the Avaya CMS software.
/usr/lib/cms/pbxtrcflags	group name <bin> expected <cms> actual	After running the Avaya CMS software.

Troubleshooting a system that fails to auto-boot

Use this procedure if the system fails to automatically pass the boot prompt (stops at the `ok` prompt). When the system reboots, a boot environment variable may be set incorrectly.

This section includes the following topics:

- Checking the boot environment variables on page 243
- Changing the boot environment variables on page 243

Checking the boot environment variables

To check the boot environment variables:

1. Enter:

   ```
   /usr/sbin/shutdown -y -g0 -i0
   ```

2. At the `ok` prompt enter:

   ```
   printenv
   ```

3. Scroll down the list and check the settings on the following variables:

   - The `auto-boot?` variable should be set to `true`.
   - The boot-device should be set to disk or to the exact system path of the RAID device which is /pci@0/pci@0/pci@9/scsi@0/disk@0,0 or /pci@0/pci@0/pci@9/LSI,mrsas@0/disk depending on the style of RAID adapter you have in your system.

Note:
The Sun Netra X4270 is an x86 based system and does NOT have eeprom variables as T5120/T5220/T4-1 systems do.

Changing the boot environment variables

To change the boot environment variables:

1. Enter:

   `setenv` ***`variable_name variable_setting`***

   Example:

   To change the `auto-boot?` variable to `true`, enter:

   ```
   setenv auto-boot? true
   ```

2. Enter:

   ```
   boot
   ```

Note:
The Sun Netra X4270 is an x86 based system and does NOT have eeprom variables as T5120/T5220/T4-1 systems do.

Diagnosing a machine panic

If a machine panic is detected on your system, you must call the TSC (domestic) or remote (international) support personnel. The TSC may request that you deliver the following information on a tape:

- Crash dump from **/var/crash/hostname/vmcore.n**
- Namelist from **/var/crash/hostname/unix.n**
- Output of the `showrev -p` command. For details, see the hardware installation document for your platform.
- Output of the `prtconf -pv` command.
- Possibly output from the **/var/adm/messages** file.

To put all of the files on one tape, do the following procedures:

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

   ```
   cd /var/crash/hostname
   ```

   The system changes to the **dump** directory.
3. Verify that **unix.n** and **vmcore.n** are present and match the date for the crash in question.
4. Enter:

   ```
   showrev -p > showrev.out
   ```

   The system retrieves the output from the **showrev -p** buffer.
5. Enter:

   ```
   dmesg > dmesg.out
   ```

   The system creates a **dmesg.out** file.
6. Enter:

   ```
   prtconf -pv>prtconf.out
   ```

   The system retrieves the output from the prtconf -pv buffer.
7. Enter:

   ```
   cp /var/adm/messages messages
   ```

   The system copies the output from the **/var/adm/messages** file.
8. Insert a tape into the default backup tape drive.

9. Enter the following command on a single line at the command prompt:

   ```
   tar cvf /dev/rmt/0 unix.X vmcore.X dmesg.out showrev.out
     prtconf.out messages
   ```

   where the letter *X* represents the number of the crashdump.

   The system displays a list of all of the files.

10. Enter the following command on a single line at the command prompt:

    ```
    rm unix.X vmcore.X dmesg.out showrev.out prtconf.out messages
    ```

    where the letter *X* represents the number of the crashdump.

    The system removes the temporary files.

11. Log out of the system.
12. Remove the tape from the disk drive and send the tape to the TSC.

Using the Sun Explorer tool

The Sun Explorer tool runs a series of tests on the system and saves the information in a tar file. This file can be sent to Sun for analysis.

> ⚠ **Important:**
> Only TSC PERSONNEL should use the Sun Explorer tool. You may be directed to use this tool per request by support personnel.

To run Sun Explorer:

1. Log in as **root**.
2. Enter the following commands:

   ```
   cd /opt/SUNWexplo/bin
   ```

   ```
   ./explorer
   ```

   The tool runs the tests and collates the information. The tar file is located in the `/opt/SUNWexplo/output` directory.
3. Support personnel will provide you with instructions on how to send the file to Sun support for analysis. This file is usually sent to Sun support by FTP. In order for Sun to analyze the file, Avaya support personnel must create a trouble ticket that includes the file name.

Using the remote console

If your system will not boot, the TSC personnel could ask you to redirect the console to the remote console so that they can identify a problem. Redirecting the console allows the TSC to dial in and do remote maintenance. You can redirect the console using *either*:

- The Solaris operating system
- OpenBoot diagnostics.

This section includes the following topics:

- Remote console ports on page 246
- Redirecting the console using Solaris on page 246
- Redirecting the console from OpenBoot mode on page 249

Remote console ports

The port used for remote console access differs, depending on the hardware platform:

Hardware platform	Port A	Port B	Port 0
Sun Enterprise T5120	Remote Console	None	None
Sun Enterprise T5220	Remote Console	None	None
Sun Netra X4270 with DigiPort USB Serial converter	None	None	Remote console

Note:
On T4-1, remote access and alarming are supported only by SAL.

Redirecting the console using Solaris

Note:
Only T5120/T5220 systems support redirection of the console.

This section describes how to use the Solaris operating system to redirect the console to serial port ttya or ttyb on an Avaya CMS system. This procedure is usually done from a remote console that has dialed in to the system.

CAUTION:
Use this procedure only when absolutely necessary. If the console redirects and the modem line drops, you may not be able to get back into the system.

This section includes the following topics:

- Redirecting the local console to the remote console on page 247
- Redirecting the remote console back to the local console on page 248

Redirecting the local console to the remote console

To redirect the local console to the remote console:

1. Dial in from the remote console to the remote console modem.
2. Log in as **root**.
3. Remove the port monitor by entering the following command at the remote console:

   `/cms/install/bin/abcadm -r ttyX`

   where ***X*** is **a** or **b**.

   The system displays the following message:

```
ttyX is currently set to be incoming

Are you sure you want to change it? [y,n,?]
```

4. At the remote console, enter: **y**

   The system displays the following message:

```
ttyX administration removed
```

5. Check the speed of the modem by entering:

   `/cms/install/bin/abcadm -k`

Note:
All remote access ports have a default speed of 9600 bps.

6. At the remote console, enter:

   `/cms/install/bin/abcadm -c -b 9600 ttyX`

   where ***X*** is **a** or **b**.

   The system displays the following message:

```
This change requires a reboot to take affect

Are you ready to reboot? [y,n,?]
```

7. At the remote console, enter: **`y`**

   The system displays the following message at the remote console:

   ```
   done
   desktop auto-start disabled
   Proceding to reboot.
   ```

   The system will automatically reboot, and the remote console port will come up as the console.

   The following occurs:

   - The system begins to shut down.
   - Shut down, reset, and reboot messages appear on the local console.
   - When the system starts to come back up, the local console goes blank.
   - The system boot diagnostics are displayed on the remote console.

   After the system reboots, a `console login:` prompt is displayed on the remote console.

8. Log into the remote console as **root**.

   The local console is blank.

   ⚠ **CAUTION:**
   Do not press **Control+D** or **`Exit`** from the remote console to exit the system without first redirecting control back to the local console. You may lock yourself from using the console locally or remotely.

Redirecting the remote console back to the local console

To redirect the console back to the local console:

1. At the remote console, enter:

   `/cms/install/bin/abcadm -c local`

   The system displays the following message:

   ```
   Console set to local

   This change requires a reboot to take affect

   Are you ready to reboot? [y,n,?]
   ```

2. At the remote console, enter: **`y`**

   The following occurs:

   - The system begins to shut down.

- Shutdown, reset, and reboot messages appear on the remote console.
- When the system starts to come back up, the system boot diagnostics are displayed on the local console.
- After the system reboots, the `console login:` prompt is displayed on the remote console.
- The login screen is displayed on the local console.

3. Log into the local console as **root**.
4. Log into the remote console as **root**.

   Control of the console port is redirected from the remote console back to the local console.

Redirecting the console from OpenBoot mode

This section describes how to use the OpenBoot mode to redirect the local console to a serial port. Use the OpenBoot mode to redirect the remote console port when the Solaris method does not work. This typically occurs when the system will not boot.

This section includes the following topics:

- Redirecting the local console to the remote console on page 249
- Redirecting the remote console back to the local console on page 250

Note:
The Sun Netra X4270 is an x86 based system and does not have eeprom variables so the system cannot redirect the console using these procedures. Additionally, although the T4-1 has eeprom variables, the console cannot be redirected since it has no native serial ports.

Redirecting the local console to the remote console

To redirect control of the console port from the local console to a dialed-in remote console:

1. If the system is not already at the `ok` prompt, enter:

   ```
   /usr/sbin/shutdown -y -i0 -g0
   ```

   The system shuts down and displays the `ok` prompt.

Note:
If the shutdown command fails, press the **Stop** + **A** keys simultaneously after the display console banner is displayed, but before the operating system starts booting.

2. At the local console, enter the following commands to set the remote console configuration parameters:

   `setenv input-device ttyX`

   `setenv output-device ttyX`

   `setenv ttyX-rts-dtr-off true`

   `setenv ttyX-ignore-cd true`

   `setenv ttyX-mode 9600,8,n,1,-`

   where *`X`* is **`a`** or **`b`**.

3. Verify the parameter changes by entering:

   `printenv`

   The system displays the following message:

```
Parameter Name        Value          Default Value
output-device         ttya           screen
input-device          ttya           keyboard
   .
   .
   .
```

4. At the local console, enter: **`boot`**

   The following occurs:

   - The system begins to shut down.
   - Shutdown, reset, and reboot messages appear on the local console.
   - When the system starts to come back up, the local console goes blank.
   - The system boot diagnostics are displayed on the remote console.
   - After the system reboots, a `console login:` prompt is displayed on the remote console.

5. Log into the remote console as **root**.

   CAUTION:
   Do not press **Ctrl** + **D** or **`exit`** from the remote console to exit the system without first redirecting control back to the local console. If you do, you may lock yourself from using the console locally or remotely.

Redirecting the remote console back to the local console

Using OpenBoot mode, there are two ways to redirect control of the console port from the remote console back to the local console:

- From the remote console (recommended)

- From the local site (not recommended)

Method 1: from the remote console

To redirect control of the console port from the remote console back to the local console:

1. Do one of the following:
   - At the remote console, if the system is in UNIX, enter the following commands:

     ```
     eeprom output-device=screen
     eeprom input-device=keyboard
     eeprom ttyX-rts-dtr-off=true
     eeprom ttyX-ignore-cd=false
     /usr/sbin/shutdown -y -i6 -g0
     ```

     where *X* is `a` or `b`.
   - At the remote console, if the system is in OpenBoot mode, enter the following commands:

     ```
     setenv output-device screen
     setenv input-device keyboard
     setenv ttyX-rts-dtr-off true
     setenv ttyX-ignore-cd false
     reset
     ```

     where *X* is `a` or `b`.

   The following occurs:

   - The system begins to shut down.
   - Shutdown, reset, and reboot messages appear on the remote console.
   - When the system starts to come back up, the system boot diagnostics are displayed on the local console.
   - The login screen is displayed on the local console.
2. At the remote console, hang up the modem connection.
3. Log into the system as **root** at the local console.
4. To see what is on the tty*X* port, enter:

   ```
   /cms/install/bin/abcadm -k
   ```
5. Start a port monitor on tty*X* by entering:

   ```
   /cms/install/bin/abcadm -i -b 9600 ttyX
   ```

   where *X* is `a` or `b`.

Method 2: from the local site

The onsite technician will use this procedure from the local site. Use this method only when Method 1 will not work.

> ⚠ **CAUTION:**
> This method of redirecting the console port should only be done as a last resort. This procedure resets the NVRAM defaults to the Sun factory settings.

To redirect control of the console port from the remote console back to the local console:

1. Cycle power on the Avaya CMS system.
2. As the computer begins to boot up, press the **Stop + N** keys simultaneously. Continue to press the **Stop + N** keys until a prompt appears on the local console.
3. At the `ok` prompt, enter: **`boot`**
4. When the system boots up, log into the system as **root** at the local console.
5. To see what is on the ttya port, enter:

   ```
   /cms/install/bin/abcadm -k
   ```

6. Start a port monitor on tty*X* by entering:

   ```
   /cms/install/bin/abcadm -i -b 9600 ttyX
   ```

   where ***X*** is **a** or **b**.

   The system displays the following message:

   ```
   ttyX set to incoming port 9600 baud
   ```

7. See the appropriate hardware installation, maintenance, and troubleshooting book for information on how to reset the NVRAM to the correct factory defaults.

Diagnosing dial-In access problems

This section describes the scenarios where the console is local and you are attempting to dial-in. It often takes a person on-site to look at the dial-in access problems.

This section includes the following topics:

- No ringing and answered responses on page 253
- Answered and connected responses do not display on page 253
- Login prompt does not display on page 254
- Login prompt is scrambled on page 256
- Remote console port will not initialize on page 257

No ringing and answered responses

Problem:

You do not get the `RINGING` and `ANSWERED` responses displayed on the screen.

Solution:

Check the following:

- Port connectivity - Refer to the hardware installation document for your platform for more details.
- Modem setup - Refer to the hardware installation document for your platform for more details.
- Serial port administration - Refer to the hardware installation document for your platform for more details.

Answered and connected responses do not display

Problem 1:

The remote dial-in does not get the `Answered` and `Connected` responses displayed on the screen.

Solution:

At the on-site location, make sure the modem is on, and check the following cabling connections:

- Phone line to the modem.
- Modem to a serial port.

Port	System
Port A	● Sun Enterprise T5120 ● Sun Enterprise T5220
Port 0[1]	● Sun Netra X4270

[1] Digi Edgeport/1, USB Serial Adapter

Note:
On T4-1, remote access and alarming are supported only by SAL.

Problem 2:

The remote user gets `Answered` and `Connected` responses displayed on the screen, but no login.

Solution:

1. Choose one of the following commands to make sure that a monitor is running:
   - **`pmadm -l; sacadm -l`**
   - **`/cms/install/bin/abcadm -k`**
2. If no port monitor is running, start a port monitor by entering:

   `/cms/install/bin/abcadm -i -b` ***`baud`*** **`tty`*****`X`***

   where ***`X`*** is **`a,`** or **`b,`** or `0`.
3. If a port monitor is running, make sure that the port monitor is set up at the correct baud rate relative to the local modem.
   - If the baud rate is not correct, remove the current port monitor and start a new port monitor at the correct baud rate. Enter the following commands:

     `/cms/install/bin/abcadm -r tty`***`X`***

     `/cms/install/bin/abcadm -i -b` ***`baud`*** **`tty`*****`X`***

     where ***`X`*** is **`a,`** or **`b,`** or `0`.
   - If the port monitor is running and is at the correct baud rate, try to fix the problem by disabling and enabling the port monitor. Enter the following commands:

     `pmadm -d -p ttymona -s tty`***`X`***

     `pmadm -e -p ttymona -s tty`***`X`***

     where ***`X`*** is **`a,`** or **`b,`** or `0`.

Login prompt does not display

Problem:

The remote user gets `Answered` and `Connected` responses displayed on the screen, but no login.

Solution:

1. Enter the following command:

   `sacadm -l`

   The system displays a message similar to the following example:

```
PMTAG          PMTYPE         FLGS RCNT STATUS     COMMAND
ttymona        ttymon         -    0    NO_SAC     /usr/lib/saf/
ttymon #Port monitor for ttya port
#
```

2. If NO_SAC displays in the STATUS column, do the following:

   a. Enter:

      `ps -ef | grep sac`

      The system displays a message similar to the following example:

```
root   278    1 0   Jan 23 ?      0:00   /usr/lib/saf/sac -t 300
root  2440 2359 0 15:27:01  pts/2 0:00   grep   sac
```

      The first number listed in the first line of the display (278 in the example above) is the process ID (PID) of the sac process.

   b. Kill the sac process by entering:

      `kill -9` ***`pid`***

      where ***`pid`*** is the process ID of sac.

      Example:

      To kill the sac process shown in **a.**, above, you would enter:

      `kill -9 278`

3. Verify that a port monitor is running by entering:

   `pmadm -l`

   The system displays the following message:

```
cms2# pmadm -l
PMTAG          PMTYPE         SVCTAG         FLGS ID
<PMSPECIFIC>
ttymona        ttymon         ttya           u    root      /dev/
term/a b - /usr/bin/login - n9600 ldterm,ttcompat login:  Port
monitor disabled - n  #CMS ttya port device
#
```

4. Check the baud rate of the port monitor (`n9600` in the example above) to make sure it is the same rate as the local modem.

5. If the baud rate is correct, go to Step 6. If the baud rate is incorrect, start a new port monitor at the correct baud rate by entering:

   ```
   /cms/install/bin/abcadm -i -b baud ttyX
   ```

   where *X* is `a,` or `b,` or `0`.

6. If the port monitor is running and is at the correct baud rate, try to fix the problem by disabling and then reenabling the port monitor. Enter the following commands:

   ```
   pmadm -d -p ttymona -s ttyX  /* disables */
   pmadm -e -p ttymona -s ttyX  /* reenables */
   ```

   where *X* is `a,` or `b,` or `0`.

Login prompt is scrambled

Problem:

The dial-in gives you scrambled characters instead of a login prompt.

Solution 1:

Try pressing a few keys to see if the problem corrects itself.

Solution 2:

If the dial-in continues to display scrambled characters instead of a login prompt, check the baud rate of the remote console by doing the following:

1. Have an on-site person run the following command:

   ```
   /cms/install/bin/abcadm -k
   ```

2. Make sure the baud rate is consistent with the modem connected on-site and the modem and console at the remote site.

3. On T5120/T5220 systems, if there is a baud rate inconsistency on-site, reconfigure the machine with the appropriate baud rate for the modem with the following command:

   ```
   /cms/install/bin/abcadm -c -b baud ttyX
   ```

   where *X* is `a` or `b.`

   The system reboots.

4. If there is a baud rate inconsistency with the remote site, reconfigure the remote site and redial.

Solution 3:

If the dial-in continues to display garbage characters instead of a login prompt, set the console back to local by switching to the local console via the OpenBoot method. See Using the remote console on page 246 for details (T5120/T5220 systems only).

Remote console port will not initialize

Problem:

The remote console port will not initialize for dialing in or dialing out.

Solution:

1. Enter:

   ```
   sacadm -l
   ```

   If the system status reports `NO_SAC`, the port is not working properly.

2. Enter:

   ```
   /cms/install/bin/abcadm -i -b 9600 ttyX
   ```

   where ***X*** is **a,** or **b,** or 0.

   This should initialize the port. If the port does not initialize, continue with Step 3.

3. Enter:

   ```
   /cms/install/bin/abcadm -r ttyX
   ```

   where ***X*** is **a,** or **b,** or **0.**

   This removes the port administration.

4. Enter:

   ```
   ps -ef | grep sac
   ```

   This finds any SAC processes that are running. If any processes are found, continue with Step 5. Otherwise, continue with Step 6.

5. Enter:

   ```
   kill -9 pid
   ```

   Use this command to kill any SAC processes still running. Process numbers are represented by ***pid***.

6. Enter:

   ```
   /usr/lib/saf/sac -t 300
   ```

   SAC restarts.

7. Enter:

   ```
   sacadm -l
   ```

   Confirm that SAC is running. The system should show `ENABLED`.

8. Enter:

   ```
   /cms/install/bin/abcadm -i -b 9600 ttyX
   ```

   where *X* is **a,** or **b,** or **0**.

   This should initialize the port.

Booting Solaris into single-user mode

This section describes how to place Solaris into single-user mode.

To boot Solaris into single user mode:

1. Log into the system through the remote console interface.
2. At the remote console, enter:

   ```
   /usr/sbin/shutdown -y -is -g0
   ```

   Note:
   The system will not successfully enter single-user mode if you execute the `shutdown` command from the local console while the console is redirected. When this occurs, the local console will not respond if you try to enter data. The remote console will also be unresponsive.

   To recover from the situation, put the system into single-user mode by performing the following procedure:

   a. Select a new window on the local console.

   b. In the new window, enter:

      ```
      /usr/sbin/shutdown -y -i0 -g0
      ```

   c. On the remote console, enter:

      ```
      boot -s
      ```

Common problems using the disc drive

Use the following procedures if you experience problems with the disc drive.

This section includes the following topics:

- Verifying that the system can read a disc on page 259
- Disc drive cannot be mounted on page 259
- Disc drive fails to open on page 259

Verifying that the system can read a disc

To verify that the system can read a disc:

- Enter:

  `mount`

  The system displays a list of devices and file systems currently mounted. The last line displayed must show the disc drive and the disc name.

  An example of a `/cdrom/`*`CD_ROMname`* message is:

```
/cdrom/CD_ROMname on /vol/dev/dsk/c0t2d0/CD_ROMname read only/nosuid/
maplcase/noglobal/rr/traildot/dev=16c0001 on current date and time
```

Disc drive cannot be mounted

If the disc drive does not respond to the mount command, the driver pointers may have been altered by the preceding `cpio` command.

To repair the driver pointers:

1. Restart the initial operating system installation.
2. When you reach the “Restore the CMSADM Backup” step, add the following to the **`cpio`** command:

   `"/dev*" "/dev*/*"`
3. Continue with the installation as you normally would.

Disc drive fails to open

If the disc drive fails to open when you press the eject button, enter the following commands:

```
cd /

eject cdrom
```

Removing the Avaya CMS package fails

Problem:

If you exited the system when removing an Avaya CMS package (cms or /cms.2), you might have:

- Logged in as **cmssvc**
- Switched users - `su'd` to **root** or **root2**
- Run **`cmssvc`**

Solution:

1. Log in directly as **root** or **root2**
2. Remove package(s) as instructed by the system.

Avaya CMS installation fails

If the Avaya CMS installation fails and the system displays the `cannot add another instance of CMS` message, either the Avaya CMS package was not removed or the removal was not completely successful.

To continue with the installation:

1. Enter:

   ```
   pkgrm cms
   ```

2. Enter:

   ```
   cd /
   ```

3. Restart the Avaya CMS installation.

CMSADM backup problems

If you receive an error message during a backup or recovery, refer to Common error messages on page 265.

As the backup progresses, the program displays a series of dots, one dot per file, to indicate it is writing files to tape. You may have a problem if you notice one of the following:

- Dots are not displaying (wait 10 minutes or longer to make certain the software is not just copying a very large file).
- The tape is not spinning.
- The system has not displayed messages prompting you to change tapes or informing you that the backup has completed.

Perform the following

- Clean the tape drive with the appropriate cleaning tape. It may be necessary to repeat this process several times.
- If the tape drive is new, clean the drive several times with the appropriate cleaning tape before use.

If you still encounter problems, call the National Customer Care Center or your product representative.

System messages

System messages can alert you to system problems, such as a device that is about to fail. By default, many of the messages are displayed on the system console and are stored in **/var/adm**.

To display system messages:

1. Enter:

   `dmesg`

   The system displays the most recent messages as shown in the following example:

```
Wed Feb 14 11:01:59 MST 2001
Feb 14 08:19:20 tern pseudo: [ID 129642 kern.info] pseudo-device: tod0
Feb 14 08:19:20 tern genunix: [ID 936769 kern.info] tod0 is /pseudo/tod@0
Feb 14 08:19:22 tern syslogd: going down on signal 15
...........
...........
...........
Feb 16 14:24:08 tern scsi: [ID 365881 kern.info] /pci@1f,0/pci@1/scsi@1,1/st@5,:
Feb 16 14:24:08 tern    <HP DDS-4 DAT (Sun)>
Feb 16 14:24:08 tern scsi: [ID 193665 kern.info] st12 at glm1: target 5 lun 0
Feb 16 14:24:08 tern genunix: [ID 936769 kern.info] st12 is /pci@1f,0/pci@1/scs0
Feb 19 10:17:59 tern automountd[198]: [ID 784820 daemon.error] server cortex nog
Feb 19 10:18:27 tern last message repeated 6 times
```

The **/var/adm** directory contains several message files. The most recent messages are in **/var/adm/messages** and in **/var/adm/messages.0**; the oldest are in **/var/adm/messages.3**. Periodically a new file is created, and the messages.3 file is deleted, messages.2 is renamed messages.3, messages.1 is renamed messages.2, and messages.0 is renamed messages.1.

The message files may contain not only system messages, but also crash dumps and other data, which can cause **/var/adm** to grow quite large. To keep the directory to a reasonable size and ensure that future crash dumps can be saved, you should remove unneeded files periodically. You can automate the task by using crontab. See your Sun system documentation for information on crontab.

Avaya CMS EEPROM settings

The following table contains the Avaya CMS EEPROM settings:

Note:
Not all options are displayed for all Avaya CMS systems. In addition, some options will show `"data not available"` messages. Ignore those options.

Option name	Required setting
ansi-terminal?	`true`
auto-boot?	`true`
boot-command	`boot`
boot-device	`disk`
diag-device	`disk`
diag-level	`min`
diag-switch?	`false`
input-device	`keyboard`
local-mac-address?	`true`
output-device	`screen`
scsi-initiator-id	`7`
ttya-ignore-cd	`false`
ttya-rts-dtr-off	`true`
ttyb-ignore-cd	`false`
ttyb-rts-dtr-off	`true`

Note:
The Sun Netra X4270 is an x86 based system and does NOT have eeprom variables as T5120/T5220/T4-1 systems do.

About RAID for CMS

The Avaya CMS system allows you to build a system with RAID 10 performance and redundancy. Having such redundancy greatly reduces the risk of data loss should a disk drive fail or your system crash.

While RAID 10 (T5120/T5220/T4-1 systems only) greatly reduces the risk of losing data, it is not meant to be a substitute for regular backups. Data can still become corrupt, and the corruption is then duplicated on the mirror.

In addition, RAID 10 (T5120/T5220/T4-1 systems only) allows for better performance through writing data across multiple disks.

Avaya CMS RAID support is enabled through a RAID controller installed in the Netra X4270, T5120, T5220 or T4-1 system. The RAID controller is then set up to use RAID 1 across 2 disks for a Netra X4270, RAID 10 across 4 disks for a T5120 4-core, and RAID 10 across 6 disks for a T5220, T5120 8-core or T4-1.

With r16.2da.i and later, two different RAID adapters are supported on the T5120/T5220 based platforms. Appropriate sections of the documentation detail specific procedures for each type of RAID adapter.

Troubleshooting problems with disk drives

Use the procedures and tips in this section to help you identify and resolve problems with:

- Physical disks
- RAID volumes
- **/cms** file system

Check the system console and the **/var/adm/messages** log for messages that indicate problems with a specific hard disk.

If a disk is generating errors, it may need to be replaced. For procedures related to recovering from disk crashes and replacing hard disk drives, see *Avaya CMS Sun SPARC Enterprise T5120/T5220 Hardware Installation, Maintenance, and Troubleshooting.*

Checking for disk recognition errors

Use these procedures to help you diagnose problems with unrecognized disk drives. This procedure differs for the different hardware platforms.

CAUTION:
Use this procedure only if the Solaris Volume Manager software indicates there is a disk recognition error.

Note:
This procedure applies only to the T5120/T5220 and T4-1 platforms.

To check for disk recognition errors:

1. Reboot the system with an `init 0` command.

   The system reboots and displays the `ok` prompt.
2. Turn off the system.
3. Turn on the system.

   When you power on the system unit, the system begins to boot.
4. Interrupt the boot by pressing **Stop** + **A**.

   The system displays the `ok` prompt.
5. Enter:

   ```
   setenv auto-boot? false
   ```

   This keeps the system from rebooting when you do a reset.

6. Enter:

   `reset-all`

   The system resets and responds with the `ok` prompt.

7. Verify that the system sees all SCSI devices by entering:

   `probe-scsi-all`

   The system displays a message that is similar to the following:

```
/pci@1f,0/pci@1/pci@5/spo@2,1

/pci@1f,0/pci@1/pci@5/scsi@2,1
Target 0
  Unit 0  Disk       QUANTUM VK4550J SUN18G8610
Target 4
  Unit 0  Removeable Tape     HP     C56P3A    C005
```

8. Verify that the RAID controller is recognized.

   If the devices are still not recognized, see the appropriate hardware installation, maintenance and troubleshooting document for more information.

9. When you have verified that the system is recognizing all of its disk drives, enter:

   `setenv  auto-boot?  true`

   CAUTION:
   If you fail to enter this command, future reboots will stop at the boot prompt instead of proceeding through the normal boot-up.

10. Enter:

    `boot -r`

    The system reboots.

11. Log in as **root**.

Common error messages

This section lists, in alphabetical order, common error messages you might encounter on an Avaya CMS system. Each message is accompanied by its probable cause and the likely solution.

- `Error in creating UNIX login for user '`*username*`'. The user may have already had UNIX log...`
  - Cause - The user already has a UNIX system login in Avaya CMS.

  - Resolution - If the user username already has a UNIX system login, ignore this message. Otherwise, verify that this user can log on and report any problems to Services.

- `ERROR: Password aging cannot be implemented on systems using NIS, NIS+ or LDAP.`
  - Cause - The system is using either NIS, NIS+ or LDAP.
  - Resolution - Contact your network administrator. The passwords will have to be aged from the server running the directory service.
- `Insufficient number of free blocks (`*#-of-blocks*`) in` *system name* `for temporary database tables.`
  - Cause - The file system does not contain enough free blocks for Avaya CMS to create the temporary tables needed for the migration.
  - Resolution - Call services to resolve this situation.
- `*** INTERNAL ERROR: contact services (`*error#, timestamp*`) ***`
  - Cause - An internal error occurred during processing of the table listed above this message.
  - Resolution - Contact services immediately. Do not remove the log file. Services needs the errornum and time stamp to find more information in their error log.
- `Request failed. See /cms/install/logdir/backup.log for more information.`
  - Cause - The tape is improperly seated in the drive, or was removed from the drive during the backup, or is write protected, or the medium is corrupted.
  - Resolution - Check the console terminal. If you see a message like WARNING: ST01: HA 0 TC 3 LU 0: Err 60503005 CMD 0000000A Sense Key 00000004 Ext Sense 00000000, the tape is corrupted. Discard it and replace it with a new tape.

    Otherwise, remove the tape from the drive and make sure it is not write protected (the black arrow in the upper left corner should be pointing away from “safe”).

    Finally, reinsert the tape into the drive, making certain it is properly seated, and restart the backup.
- `UNRECOVERABLE ERROR READING TAPE, errno= Failed to open tape: no entry in the device directory. Make sure the Maintenance: Backup/Restore Devices screen has the correct Path.`
  - Cause - The program could not open the tape drive to read the Avaya CMS data.
  - Resolution - Check that the specified tape drive is set up with the correct path in the `Maintenance: Backup/Restore Devices` window. If you cannot resolve this problem, contact services for additional help. You may have a tape drive hardware problem or need a corrected tape device path.
- `** WARNING:** Only one user may run age_pw at one time.`

  - Cause - More than one person is attempting to use the `passwd_age` option in the CMSADM menu.
  - Resolution - Attempt to run the command after a few minutes have passed. If you still receive the warning message, contact Avaya CMS services.
- `You must be root in order to run this command.`
  - Cause - Superuser privileges are necessary to run this script because most of the commands are related to system administration.
  - Resolution - Log in as the root user and rerun the command.
- `/etc/system has been updated since the last reboot. CMS cannot run without an up-to-date /etc/system file.`
  - Cause - **/etc/system** can change when a particular Solaris patch is applied to the system or when state database replicas are removed and re-added during a boot disk replacement.
  - Resolution - Reboot the system.
- `filename restored from filebackup`
  - Cause - The action failed, and the **md.tab** file was restored from the previous version. Consequently, the configuration files reflect the previous system setup.
  - Resolution - Determine the cause of the problem and try again.
- `stale databases`
  - Cause - The state database contains old information.
  - Resolution - Recreate the database.
- `syntax error`
  - Cause - The syntax and usage of the command may be incorrect.
  - Resolution - Reenter the command, correcting syntax errors you have made.
- `The file` *filename* `could not be restored.`
  - Cause - The previous action failed, and the **md.tab** file or **vfstab** file could not be copied back. The existing files may not accurately reflect the system environment.
  - Resolution - Check the file and repair it if necessary.
- `The /cms filesystem needs to be mounted`
  - Cause - /cms must be mounted for the command to work.
  - Resolution - Mount /cms with the command:

    ```
    mount /cms
    ```
- `This command may hang the system if a Stop+A or halt command has been executed. Please type reset-all to reset the system before executing this command. Do you wish to continue?`
  - Resolution - Perform the following procedure:

a. Prevent the probe from continuing by entering:

   ```
   N
   ```

b. Prevent the system from rebooting by entering:

   ```
   setenv  auto-boot?  false
   ```

c. Enter:

   ```
   reset-all
   ```

   The reset may take a minute to complete. Once it does, you may do the **`probe-scsi`** or **`probe-scsi-all`** and perform any other boot prom level diagnostics.

d. Before you reboot again, enter:

   ```
   setenv  auto-boot?  true
   ```

   Failure to do so will cause the reboot to stop at the boot prompt.

- `touch: /cms/db/unix_start cannot create`
  - Cause - A CMSADM backup was done when Avaya CMS was still running. An attempt is made to restart Avaya CMS, but Avaya CMS files are not yet available.
  - Resolution - No response required. The message will disappear after you have restored and migrated Avaya CMS.

-
  ```
  Warning: inode blocks/cyl group (230 >= data blocks (135) in lost
  cylinder group.  This implies 2160 sector(s) cannot be allocated.
  ```
  - Resolution - Some sectors will not be used by the filesystem. This is just a warning; the filesystem should be fine.
- `logtime[xxx]: Failed to list SAVECORE dir contents. ERROR 0`
  - Resolution – No action required, this is an informational message only indicating that no coredump files currently exist.

Report Query Status

Two types of report query logs are being added with release R16.2. These logs track the queries made by historical reports and they show the queries that have completed and the queries that are currently being run. This information can be used to determine who is running what reports and if those report queries are affecting system performance.

Information about query logs

- Types of report query logs:
  - qlog: a log where entries are made upon query completion
  - idbm log: a log showing the query that is currently running
- These logs are always in operation implying that they do not need to be turned off/on
- Comparison between the report query logs
  - qlog has more detail, but is only updated after the report query has completed
  - idbm log shows currently running queries and is updated at completion of the query to add completion status
- Uses of report query logs
  - qlog can show past report execution to determine who ran queries and how long the queries took
  - idbm log can be used to determine what queries are running currently. This can be used to determine if a particular query is taking a long time and thus negatively impacting system performance.
  - Log information in either logs cannot be used to kill a particular report; it is debug information only
- qlog features
  - Entries are made upon query/report completion
  - Applies to historical report queries only
  - Log entries have information about start time, user, run time, completion status, task ID and query text
  - qlogs are store in directory `/cms/db/log` as `qlog, qlog.01, qlog.02`, etc.
  - The size and number of qlog files are administered in the file `/cms/db/LogAdmin/qlog` on the server
  - Example entry:

```
Mon Sep 13 00:35:50 2010 USER=dsb123    TIME=00:00 STATUS=0     TASK=13018
QUERY=select vdn, starttime, intrvl, acdcalls, acdtime, abncalls,
busycalls,disccalls,incalls,othercalls from hvdn where row_date = 40432
and acd = 1  order by vdn, starttime
```

- idbm log features
  - Entries are made for currently running queries.
  - Applies to historical report queries only.

- IDBM stands for Informix Database Manager. These are the processes that interface with the historical database.
- log entries contain information about start time, user and query text.
- The idbm logs are kept in the server in directory `/cms/db/log` as idbm.'process ID'. For example: `idbm.17, idbm.1001, idbm.13027`, etc.
- Example entry:

```
Tue Sep 14 16:32:33 2010 dsb123 select value, item_name from synonyms
where item_type='split' and acd_no=1
```

- If no query is running in that idbm process, the log will show the last query run along with its status.
- Example status entry:

```
Tue Sep 14 16:32:33 2010 STATUS=0
```

Troubleshooting Visual Basic Errors

The following table describes some of the Visual Basic errors seen while running Avaya CMS Supervisor:

Error code	Error Message
3	Return without GoSub
5	Invalid procedure call
6	Overflow
7	Out of memory
9	Subscript out of range
10	This array is fixed or temporarily locked
11	Division by zero
13	Type mismatch
14	Out of string space
16	Expression too complex
17	Can't perform requested operation

Error code	Error Message
18	User interrupt occurred
20	Resume without error
28	Out of stack space
35	Sub, function, or property not defined
47	Too many DLL application clients
48	Error in loading DLL
49	Bad DLL calling convention
51	Internal error
52	Bad file name or number
53	File not found
54	Bad file mode
55	File already open
57	Device I/O error
58	File already exists
59	Bad record length
61	Disk full
62	Input past end of line
63	Bad record number
67	Too many files
68	Device unavailable
70	Permission denied
71	Disk not ready
74	Can't rename with different drive
75	Path/File access error
76	Path not found
91	Object variable or With block variable not set
92	For Loop not initialized

Error code	Error Message
93	Invalid pattern string
94	Invalid use of Null
298	System DLL could not be loaded
320	Can't use character device names in specified file names
321	Invalid file format
322	Can't create necessary temporary file
325	Invalid format in resource file
327	Data value named was not found
328	Illegal parameter; can't write arrays
335	Could not access system registry
336	ActiveX component not correctly registered
337	ActiveX component not found
338	ActiveX component did not correctly run
360	Object already loaded
361	Can't load or unload this object
363	Specified ActiveX control not found
364	Object was unloaded
365	Unable to unload within this context
368	The specified file is out of date. This program requires a newer version
371	The specified object can't be used as an owner form for Show
380	Invalid property value
381	Invalid property-array index
382	Property Set can't be executed at run time
383	Property Set can't be used with a read-only property
385	Need property-array index

Error code	Error Message
387	Property Set not permitted
393	Property Get can't be executed at run time
394	Property Get can't be executed on write-only property
400	Form already displayed; can't show modally
402	Code must close topmost modal form first
419	Permission to use object denied
422	Property not found
423	Property or method not found
424	Object required
425	Invalid object use
429	ActiveX component can't create object or return reference to this object
430	Class doesn't support OLE Automation
430	Class doesn't support Automation
432	File name or class name not found during Automation operation
438	Object doesn't support this property or method
440	OLE Automation error
440	Automation error
442	Connection to type library or object library for remote process has been lost
443	Automation object doesn't have a default value
445	Object doesn't support this action
446	Object doesn't support named arguments
447	Object doesn't support current locale settings
448	Named argument not found
449	Argument not optional or invalid property assignment

Error code	Error Message
450	Wrong number of arguments or invalid property assignment
451	Object not a collection
452	Invalid ordinal
453	Specified DLL function not found
454	Code resource not found
455	Code resource lock error
457	This key is already associated with an element of this collection
458	Variable uses a type not supported in Visual Basic
459	This component doesn't support events
460	Invalid Cipboard format
461	Specified format doesn't match format of data
480	Can't create AutoRedraw image
481	Invalid picture
482	Printer error
483	Printer driver does not support specified property
484	Problem getting printer information from the system. Is printer is set up correctly?
485	Invalid picture type
486	Can't print form image to this type of printer
735	Can't save file to Temp directory
744	Search text not found
746	Replacements too long
31001	Out of memory
31004	No object
31018	Class is not set
31027	Unable to activate object
31032	Unable to create embedded object

Error code	Error Message
31036	Error saving to file
31037	Error loading from file

You can try out the following steps towards resolving these errors:

1. Log out and log in back again.
2. If the error is still there, reboot the PC on which the VB error is occuring.
3. Find out if the error is occuring on any other PC on which CMS Supervisor is installed.
4. If the error is occuring on only one PC, reinstall CMS Supervisor.
5. If the error still does not go away, contact Avaya Global Support Services.

Glossary

ACD See Automatic call distribution (ACD) on page 277.

Agent A person who answers calls to an extension in an ACD split. This person is known to CMS by a login identification keyed into a voice terminal.

Agent skill The different types of calls a particular agent can handle. An agent can be assigned up to four skills. These skills are assigned as either primary or secondary skills. For more information, see Primary skill on page 280 or Secondary skill on page 280.

Agent state A feature of agent call handling that allows agents to change their availability to the system (for example, ACW, AVAIL, ACD).

Automatic call distribution (ACD) A switch feature. ACD is software that channels high-volume incoming call traffic to agent groups (splits or skills).

Also an agent state where the extension is engaged in an ACD call (with the agent either talking to the caller or the call waiting on hold).

Avaya Call Management System (CMS) A software product used by business customers that have a Lucent Technologies telecommunications switch and receive a large volume of telephone calls that are processed through the ACD feature of the switch.

Boot To load the system software into memory and start it running.

Call Vectoring A highly flexible method for processing ACD calls using Vector Directory Numbers (VDNs) and vectors as processing points between trunk groups and splits or skills. Call vectoring permits treatment of calls that is independent of splits or skills.

CMS Call Management System. See Avaya Call Management System (CMS) on page 277.

CMSADM menu The Call Management System Administration (CMSADM) menu allows a user to administer features of CMS.

CMSADM file system backup A backup that saves all the file systems on the machine which includes the Solaris operating system and programs, CMS programs and data, and non-CMS data you place on the computer in addition to the CMS data.

CMSSVC menu The Call Management System Services (CMSSVC) menu allows support personnel to manage CMS system services.

Common Desktop Environment A desktop user interface for Solaris.

Configuration Configuration is the way that the computer is set up to allow for particular uses or situations.

Custom reports Real-time or historical reports that have been customized from standard reports or created from original design.

Data collection off CMS is not collecting ACD data. If you turn off data collection, CMS will not collect data on current call activity.

Data backup The backup that uses ON-Bar to backup the CMS Informix data. This is used with the CMS LAN backup feature.

Database A group of files that store ACD data according to a specific time frame: current and previous intrahour real-time data and intrahour, daily, weekly, and monthly historical data.

Database item A name for a specific type of data stored in one of the CMS databases. A database item may store ACD identifiers (split numbers or names, login IDs, VDNs, and so on) or statistical data on ACD performance (number of ACD calls, wait time for calls in queue, current states of individual agents, and so on).

Database tables Tables that CMS uses to collect, store, and retrieve ACD data. Standard CMS items (database items) are names of columns in the CMS database tables.

Device The term used to refer to the peripheral itself; for example, a hard disk or a tape drive. A peripheral is sometimes referred to as a subdevice or an Logical Unit (LU).

EAD See Expert Agent Distribution (EAD) on page 278.

EAS See Expert Agent Selection (EAS) on page 278.

Error message An error message is a response from a program indicating that a problem has arisen or something unexpected has happened, requiring your attention.

Ethernet A type of network hardware that allows communication between systems connected directly together by transceiver taps, transceiver cables, and a coaxial cable. Also implemented using twisted-pair telecommunications wire and cable.

Ethernet address A unique number assigned to each system when it is manufactured. The Ethernet address of your system is displayed on the banner screen that appears when you power on your system.

Exception A type of activity on the ACD which falls outside of the limits the customer has defined. An exceptional condition is defined in the CMS Exceptions subsystem, and usually indicates abnormal or unacceptable performance on the ACD (by agents, splits or skills, VDNs, vectors, trunks, or trunk groups).

Expert Agent Distribution (EAD) A call queued for a skill will go to the most idle agent (primary skill agent). Agents who are idle and have secondary agent skills will receive the call queued for a skill if there are no primary agents available.

Expert Agent Selection (EAS) An optional feature that bases call distribution on agent skill (such as language capability). EAS matches the skills required to handle a call to an agent who has at least one of the skills required.

Forecast reports These reports display expected call traffic and agent or trunk group requirements for the customer’s call center for a particular day or period in the future.

Historical database Contains intrahour records for up to 62 days in the past, daily records for up to 5 years in the past, and weekly or monthly records for up to 10 years for each CMS-measured agent, split or skill, trunk, trunk group, vector, and VDN.

Historical reports Reports that display past ACD data for various agent, split or skill, trunk, trunk group, vector, or VDN activities.

Host computer A computer that is attached to a network and provides services other than simply acting as a store-and-forward processor or communication switch.

Host name A name that you (or your system administrator) assign to your system unit to uniquely identify it to the Solaris 9 operating system (and also to the network).

IDS See Informix Dynamic Server (IDS) on page 279.

Informix Dynamic Server (IDS) A relational database management system used to organize CMS data. An add-on software package needed by CMS.

Interface A common boundary between two systems or pieces of equipment.

Link A transmitter-receiver channel or system that connects two locations.

Log in The process of gaining access to a system by entering a user name and, optionally, a password.

Log out The process of exiting from a system.

Measured A term that means an ACD element (agent, split or skill, trunk, trunk group, vector, VDN) has been identified to CMS for collection of data.

Multi-user mode A mode of CMS in which any administered CMS user can log into CMS. Data continues to be collected if data collection is “on.”

Network address A unique number assigned to each system on a network, consisting of the network number and the system number. Also known as Internet Address or Internet Protocol (IP) address.

Non-volatile random access memory (NVRAM) A random access memory (RAM) system that holds its contents when external power is lost.

NVRAM See Non-volatile random access memory (NVRAM) on page 279.

Operating system (OS) The software that controls and allocates the resources, such as memory, disk storage, and the screen display for the computer.

Partitions Sections of the hard disk that are used to store an operating system and data files or programs. By dividing the disk into partitions, you can use the space allocated in a more efficient and organized manner.

Password A character string that is associated with a user name. Provides security for a user account. Desktop computers require you to type a password when you log into the system, so that no unauthorized person can use your system.

Port (I/O port) A designation of the location of a circuit that provides an interface between the system and lines and/or trunks.

Primary skill An agent will handle calls to many skills before calls to secondary skills.

Screen labeled key (SLK) The first eight function keys at the top of the keyboard that correspond to the screen labels at the bottom of the terminal screen. The screen labels indicate the function each key performs.

SCSI See Small computer system interface (SCSI) on page 280.

Secondary skill An agent will handle secondary skill calls after primary skill calls.

Serial asynchronous interface/PCI A card that provides access to eight serial ports by connecting to an eight-port patch panel.

Single-user mode A CMS mode in which only one person can log into CMS. Data collection continues if data collection is “on.” This mode is required to change some CMS administration.

Skill In relationship to the call center, think of skill as a specific customer need or requirement, or perhaps a business need of the call center.

SQL See Structured Query Language (SQL) on page 280.

Slot An electronic connection designed to receive a module or a printed circuit board (such as a Single In-line Memory Module [SIMM] or a frame buffer board).

Small computer system interface (SCSI) A hardware interface that allows the connection of peripheral devices (such as hard disks, tape drives and disc drives) to a computer system.

Split A group of extensions that receive special-purpose calls in an efficient, cost-effective manner. Normally, calls to a split arrive over one or a few trunk groups.

Storage device A hardware device that can receive data and retain it for subsequent retrieval. Such devices cover a wide range of capacities and speeds of access.

Structured Query Language (SQL) A language used to interrogate and process data in a relational database. SQL commands can be used to interactively work with a database or can be embedded within a programming language to interface to a database.

Super-user A user with full access privileges on a system, unlike a regular user whose access to files and accounts is limited.

Switch A private switch system providing voice-only or voice and data communications services (including access to public and private networks) for a group of terminals within a customer’s premises.

Syntax The format of a command line.

System A general term for a computer and its software and data.

System backup The backup that uses a storage manager to backup the UNIX files. This is used with the CMS LAN backup feature.

Tape cartridge A magnetic piece of hardware that is used as a storage unit for data.

TCP/IP See Transmission control protocol/internet protocol (TCP/IP) on page 281.

Technical Service Center (TSC) The Avaya organization that provides technical support for Avaya products.

TSC See Technical Service Center (TSC) on page 281.

Transmission control protocol/ internet protocol (TCP/IP) A communications protocol that provides interworking between dissimilar systems.

Trunk A telephone line that carries calls between two switches, between a Central Office (CO) and a switch, or between a CO and a phone.

Trunk group A group of trunks that are assigned the same dialing digits - either a phone number or a Direct Inward Dialing (DID) prefix.

UNIX system The operating system on the computer on which CMS runs. Sun Microsystems uses Solaris as its UNIX operating system.

User ID The login ID for a CMS user.

User name A combination of letters, and possibly numbers, that identifies a user to the system.

VDN See Vector directory number (VDN) on page 281.

Vector A list of steps that process calls in a user-defined manner. The steps in a vector can send calls to splits, play announcements and/or music, disconnect calls, give calls a busy signal, or route calls to other destinations. Calls enter vector processing by way of VDNs, which may have received calls from assigned trunk groups, from other vectors, or from extensions connected to the switch.

Vector directory number (VDN) An extension number that is used in ACD software to permit calls to connect to a vector for processing. A VDN is not assigned an equipment location; it is assigned to a vector. A VDN can connect calls to a vector when the calls arrive over an assigned automatic-in trunk group or when calls arrive over a dial-repeating (DID) trunk group, and the final digits match the VDN. The VDN by itself may be dialed to access the vector from any extension connected to the switch.

Index