Avaya Call Management System
Release 13
CMS Upgrade Express (CUE)
Customer Requirements
Providing telecommunications security

Telecommunications security (of voice, data, and video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or person working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either toll through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Use (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including, but not limited to, human and data privacy, intellectual property, material assets, financial resources, labor costs, and legal costs).

Your responsibility for your company's telecommunications security

The final responsibility for securing both this system and its networked equipment rests with you, an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources, including, but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products.

Avaya Publications Center

Voice: +1-207-866-6701
1-800-457-1764 (Toll-free, U.S. and Canada only)

Fax: +1-207-626-7269
1-800-457-1764 (Toll-free, U.S. and Canada only)

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Manager

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

E-mail: totalware@gwsmail.com

Order: Material ID 700356744, Issue 1.0
May 2005

For the most current versions of documentation, go to the Avaya support Web site:

http://www.avaya.com/support

COMPAS

This document is also available from the COMPAS database. The COMPAS ID for this document is 106994.

Avaya support

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

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

Preface .................................................. 5
  Related documents .................................. 5
  Support ................................................. 6

Procedures required before the upgrade .................................. 7
  Who must do upgrades ................................ 8
  Collecting the upgrade kit and extra disks ...................... 8
  Cleaning the tape drive ................................ 8
  Doing a CMSADM backup ................................ 9
  Doing a full maintenance backup ............................. 12
  Doing an incremental maintenance backup ...................... 13
  Collecting third-party and custom software ..................... 14

Procedures required after the upgrade .................................. 15
  Checking the manual merge files ........................... 16
  Verifying CMS security ................................ 16
  Migrating historical data ................................. 16
  Restoring non-CMS files (optional) ......................... 18
  Installing and administering unpreserved software ........... 19
  Doing a CMSADM backup ................................ 20
  Doing a full maintenance backup ........................... 20
Preface

Avaya Call Management System (CMS) Release 13 CMS Upgrade Express (CUE)
Customer Requirements is written for customers who are preparing to have their CMS computer upgraded from CMS R3V9, R3V11, R12, or R13 to the latest CMS R13 software.

Note:
CUE cannot be used to upgrade a Sun SPARCserver computer, Sun Ultra 5 computer, Sun Enterprise 3000 computer, or Sun Enterprise 3500 computer to R13. Also, CUE cannot be used to upgrade a CMS R3V8 or earlier system to R13. You must follow the procedures found in Avaya CMS Release 13 Platform Upgrade and Data Migration.

Related documents

The following table lists the CUE upgrade documents. These documents are shipped with CUE upgrade kits.

<table>
<thead>
<tr>
<th>Title</th>
<th>Document number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya CMS R13 Sun Blade 100/150 Workstation Mirrored and Nonmirrored Systems CUE</td>
<td>07-300481</td>
</tr>
<tr>
<td>Avaya CMS R13 Sun Fire V880/V890 Computer CUE</td>
<td>07-300344</td>
</tr>
</tbody>
</table>

Subsequent updates are available on the Avaya support web site.
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.
Procedures required before the upgrade

It is the customer’s responsibility to ensure that the following procedures are done before the upgrade starts. Use the following checklist to verify that the procedures are done.

<table>
<thead>
<tr>
<th>Procedure</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Who must do upgrades on page 8</td>
<td>✓</td>
</tr>
<tr>
<td>Collecting the upgrade kit and extra disks on page 8</td>
<td></td>
</tr>
<tr>
<td>Cleaning the tape drive on page 8</td>
<td></td>
</tr>
<tr>
<td>Doing a CMSADM backup on page 9</td>
<td></td>
</tr>
<tr>
<td>Doing a full maintenance backup on page 12</td>
<td></td>
</tr>
<tr>
<td>Doing an incremental maintenance backup on page 13</td>
<td></td>
</tr>
<tr>
<td>Collecting third-party and custom software on page 14</td>
<td></td>
</tr>
</tbody>
</table>
Who must do upgrades

Upgrades are done by Avaya-authorized personnel based on the following conditions:

- In the United States and Canada, only Avaya CMS Provisioning personnel do upgrades. Avaya CMS Provisioning is assisted by on-site Avaya technicians.
- Outside the United States and Canada, Avaya-approved business partners or system integrators do upgrades.

⚠️ Important:
If nonauthorized personnel do these procedures, the following consequences can occur:
- You might permanently lose data.
- The CMS system might be put in a nonfunctioning state for some time.
- You might be charged additional time and material expenses by Avaya.

Collecting the upgrade kit and extra disks

Verify that the CUE kit and any extra data disks were received. Store the kit and data disks with the system being upgraded.

Cleaning the tape drive

See your Sun computer hardware documentation for instructions on how to clean the tape drive.

⚠️ Important:
CMS R13 supports only the following tape drives:
- 20/40 GB 4mm DDS-4
- 36/72 GB 4mm DAT 72

If you do not have one of these tape drives, your system is probably incompatible and cannot support a CUE upgrade to R13. You must do a platform upgrade as described in Avaya CMS Release 13 Platform Upgrade and Data Migration.
Doing a CMSADM backup

A recent CMSADM backup is required before starting any upgrade. For best results, do a CMSADM backup the night before the upgrade. Minimally, the CMSADM backup must not be *more* than a week old. Check the backup log at `/cms/install/logdir/backup.log` for the date of the last CMSADM backup.

To do a CMSADM backup:

⚠️ **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.

1. Log on as root.
2. Enter:
   ```
   cmsadm
   ```
   The CMS Administration menu is displayed.
3. Enter the number that corresponds to the `backup` option.
   Depending on the configuration of your system, one of the following options are displayed:
   - If only one tape drive is available on the system, the following messages are displayed:
     ```
     Please insert the first cartridge tape into <device name>.
     Press ENTER when ready or Del to quit:
     ```
     Continue with Step 5.
   - If more than one tape drive is available for use by the system, a message listing the different tape drives is displayed.
4. Enter a tape drive selection from the displayed list.
   The following messages are displayed:
   ```
   Please insert the first cartridge tape into <device name>.
   Press ENTER when ready or Del to quit:
   ```
Procedures required before the upgrade

5. Press **Enter**.

   The backup process starts. If more than one tape is required, the following messages are displayed:

   End of medium on "output".
   Please remove the current tape, number it, insert tape number x, and press Enter

6. If the message in Step 5 is displayed, insert the next tape and allow it to rewind. When it is properly positioned, press **Enter**.

7. When the backup is completed, information according to the number of tapes that are required for the backup is displayed:

   - If the number of tapes required is one, the following messages are displayed:

     xxxxxxxx blocks
     Tape Verification
     xxxxxxxx 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 (R3VXxx.x)

     Continue with Step 12.

   - If the number of tapes required is more than one, the following messages are displayed:

     xxxxxxxx blocks
     Tape Verification
     Insert the first tape
     Press Return to proceed:

8. Insert the first tape to be used for the backup.

9. Press **Enter**.

10. When the LED on the tape drive stops blinking, remove the tape.

11. When prompted, repeat Step 8 for any additional tapes generated by the backup process. When the final tape is verified, the following messages are displayed:

     xxxxxxxx blocks
     Tape Verification
     xxxxxxxx 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 (R3VXxx.x)
12. Label all tapes with the:
   ● Tape number
   ● Date of backup
   ● Current version of CMS
13. Set the tape write-protect switch to read-only.
A full maintenance backup provides migration data for the new CMS version. Do the backup the night before the upgrade. Backups are done using the CMS Backup Data window.

To do a full maintenance backup:

1. Log on to CMS.

2. Select **Maintenance > Back Up Data** from the CMS main menu.

   The **Backup Data** window is displayed.

3. In the **Backup Data** window, select the options and enter the values that are indicated in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value to enter or option to select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device name</td>
<td>The tape drive device name</td>
</tr>
<tr>
<td>Verify tape...?</td>
<td>y</td>
</tr>
<tr>
<td>ACD(s) to back up</td>
<td>All ACDs</td>
</tr>
<tr>
<td>Data to back up</td>
<td>Local system administration data</td>
</tr>
<tr>
<td></td>
<td>CMS system administration data</td>
</tr>
<tr>
<td></td>
<td>ACD-specific administration data</td>
</tr>
<tr>
<td></td>
<td>Historical data - Full</td>
</tr>
<tr>
<td></td>
<td>Non-CMS data (if needed)</td>
</tr>
</tbody>
</table>

4. Press **Enter** to access the action list, and select **Run**.

5. After the backup is complete, remove the backup tape.

6. Label the tape with the date and note that it is a full backup.
Doing an incremental maintenance backup

Do an incremental maintenance backup immediately before the upgrade.

⚠️ Important:
To back up the most recent set of data, ensure that you start the backup after the data collection archiving interval.

To do an incremental maintenance backup:

1. Log on to CMS.
2. Select Maintenance > Back Up Data from the CMS main menu.
   The Backup Data window is displayed.
3. In the Backup Data window, select the options and enter the values that are indicated in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value to enter or option to select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device name</td>
<td>The tape drive device name</td>
</tr>
<tr>
<td>Verify tape...?</td>
<td>y</td>
</tr>
<tr>
<td>ACD(s) to back up</td>
<td>All ACDs</td>
</tr>
<tr>
<td>Data to back up</td>
<td>Local system administration data CMS system administration data ACD-specific administration data Historical data - Incremental Non-CMS data (if needed)</td>
</tr>
</tbody>
</table>

4. Press Enter to access the action list, and select Run.
5. After the backup is complete, remove the backup tape.
6. Label the tape with the date and note that it is an incremental backup.
Collecting third-party and custom software

If third-party, custom software, or other Avaya products are installed on the system, the customer must gather that software so it will be available for installation after the upgrade. This can include software such as Operational Analyst or information about pseudo-ACDs. After the upgrade, either Avaya Provisioning or Avaya Communication Solutions and Integration (CSI) will reinstall this software.
Procedures required after the upgrade

After the upgrade is completed, the customer must do the following procedures to restore the system to normal operation:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking the manual merge files</td>
<td>16</td>
</tr>
<tr>
<td>Verifying CMS security</td>
<td>16</td>
</tr>
<tr>
<td>Migrating historical data</td>
<td>16</td>
</tr>
<tr>
<td>Restoring non-CMS files (optional)</td>
<td>18</td>
</tr>
<tr>
<td>Installing and administering unpreserved software</td>
<td>19</td>
</tr>
<tr>
<td>Doing a CMSADM backup</td>
<td>20</td>
</tr>
<tr>
<td>Doing a full maintenance backup</td>
<td>20</td>
</tr>
</tbody>
</table>

The customer can contract with Avaya CSI or CMS Provisioning to do any or all of these procedures.
Procedures required after the upgrade

Checking the manual merge files

The customer must look at the files saved in the /manual_merge directory. The customer must determine if any differences are Solaris changes which should not be modified or customer customization changes which might need to be modified. The identified files might be important to the new system. The customer might find that these files need to be copied to a location that might eventually fix a problem. These files might contain networking information, customizations, or security settings that are critical to the customer.

For more information about manual merge discrepancies, see your Avaya upgrade representative.

Verifying CMS security

If you had previously applied CMS security procedures to your system, those procedures must be redone for the new version of Solaris. Contact your Avaya account representative or support organization and ask for the document “Customer Procedures For Securing the CMS.”

Migrating historical data

After migrating the system administration data and the agent and call center administration data, you must migrate the historical data. You must migrate the historical data twice. Use the full backup tape first, followed by the incremental backup tape.

To migrate historical data:

1. Log on to CMS.
   
   The CMS main menu is displayed.

2. Verify that the maintenance backup tape is in the tape drive. Use the most recent full backup first, followed by the most recent incremental backup.

3. From the CMS main menu, select System Setup > R3 Migrate Data.
   
   The R3 Migrate Data window is displayed.
4. In the **R3 Migrate Data** window, select the options and enter the values that are indicated in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value to enter or option to select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device name</td>
<td>The tape drive device name</td>
</tr>
<tr>
<td>Data Type</td>
<td>Historical data</td>
</tr>
<tr>
<td>Stop date</td>
<td>Leave blank</td>
</tr>
<tr>
<td>Stop time</td>
<td>11:59 PM</td>
</tr>
<tr>
<td>Specify ACD(s)</td>
<td>All ACDs</td>
</tr>
</tbody>
</table>

5. Press **Enter** to access the action list in the top right corner.

6. Select **Run** and press **Enter**.

   The progress of the migration is displayed in the **Status** field. When the migration ends, the system indicates the success or failure of the migration in this field.

   Note that a full historical migration can take several hours. It runs in the background, however, so you can exit the migration window and perform other tasks. If you do that, bring up the migration window periodically to check on the progress.

7. Press **F3** and select the UNIX option to display the UNIX prompt.

8. Enter:

   `pg /cms/migrate/r3mig.log`

   The customer migration log is displayed.

9. Look at the contents of the customer migration log and take any necessary corrective action. For help with interpreting the log, contact technical support or your customer representative.

10. To exit the UNIX window, enter:

    `exit`
Restoring non-CMS files (optional)

The customer might want specific non-CMS files copied from the preupgrade CMSADM backup tape to the upgraded system.

To copy specific files from one system to another:

1. Insert the most recent CMSADM backup tape from the old system into the tape drive.
2. Enter:
   ```
   cd /
   ```
3. Enter the following command for each file you want to copy:
   ```
   cpio -icmudv -C 10240 -I /dev/rmt/X -M "Remove current tape, insert tape number %d, press ENTER" "<path>/<file_name>"
   ```
   The `<path>/<file_name>` is the relative path to the file being copied.
   
   The X is either 0 or 1, depending on how many tape drives are connected to the system. If you have only one tape drive, use 0. If you have more than one tape drive, use the following commands to determine which tape drive can be used:
   ```
   mt -f /dev/rmt/0 status
   mt -f /dev/rmt/1 status
   ```
   The tape drive that contains the CMSADM backup tape reports a status similar to the following example:

   ```
   <tape drive model name>:
   sense key(0x6)= Unit Attention residual= 0 retries= 0
   file no= 0 block no= 0
   ```

   For example, a command to copy the file `/accounting/invoices` is:
   ```
   cpio -icmudv -C 10240 -I /dev/rmt/X -M "Remove current tape, insert tape number %d, press ENTER" "accounting/invoices"
   ```
Installing and administering unpreserved software

After the upgrade, you must contract with Avaya to install any unpreserved software and administer any new features or services. The following table lists several of these features and services and the Avaya organizations that are responsible for completing the work.

<table>
<thead>
<tr>
<th>Feature or service</th>
<th>Responsible^1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Call Center</td>
<td>CSI</td>
</tr>
<tr>
<td>Operation Analyst, including restarting forwarders</td>
<td>CSI</td>
</tr>
<tr>
<td>Network information names service, such as NIS or NISplus</td>
<td>CSI</td>
</tr>
<tr>
<td>Network printers</td>
<td>CSI</td>
</tr>
<tr>
<td>Pseudo-ACDs. Pseudo-ACDs must be added and data must be migrated from the old system.</td>
<td>CSI</td>
</tr>
<tr>
<td>Applications such as workforce management software</td>
<td>CSI</td>
</tr>
<tr>
<td>Wallboards</td>
<td>CSI</td>
</tr>
<tr>
<td>Mounted file systems that were in the customer’s /etc/vfstab file before the upgrade. See the copy of /etc/vfstab that is saved in /var/log/cvuelog. Have your administrator verify that your new configuration is correct.</td>
<td>Provisioning</td>
</tr>
<tr>
<td>Common Desktop Environment options such as screen layout and password protection</td>
<td>Provisioning</td>
</tr>
<tr>
<td>Add, change, or remove ACDs</td>
<td>Provisioning</td>
</tr>
<tr>
<td>Add Supervisor logins</td>
<td>Provisioning</td>
</tr>
<tr>
<td>Install new feature packages (if purchased)</td>
<td>Provisioning</td>
</tr>
<tr>
<td>Change authorizations</td>
<td>Provisioning</td>
</tr>
<tr>
<td>Start up the Alarm Origination Manager (AOM) software</td>
<td>Provisioning</td>
</tr>
<tr>
<td>Reconfigure the Remote System Control (RSC) card on the Sun Fire V880/V890</td>
<td>Customer</td>
</tr>
<tr>
<td>Update security options such as rsh and rlogin.</td>
<td>Customer</td>
</tr>
</tbody>
</table>

^1. Outside the United States, Avaya distributors are responsible for these items, with assistance from the COE.
Doing a CMSADM backup

Do a CMSADM backup on the system as described in Avaya CMS R13 Software Installation, Maintenance and Troubleshooting. If LAN Backup is being used on the new system, see Avaya CMS R13 LAN Backup User Guide.

Doing a full maintenance backup

A full maintenance backup provides migration data for the new CMS version. Backups are done using the CMS Backup Data window.

To do a full maintenance backup:

1. Log on to CMS.
2. Select Maintenance > Back Up Data from the CMS main menu.
   
   The Backup Data window is displayed.
3. In the Backup Data window, select the options and enter the values that are indicated in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value to enter or option to select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device name</td>
<td>The tape drive device name</td>
</tr>
<tr>
<td>Verify tape...?</td>
<td>y</td>
</tr>
<tr>
<td>ACD(s) to back up</td>
<td>All ACDs</td>
</tr>
<tr>
<td>Data to back up</td>
<td>Local system administration data CMS administration data ACD-specific administration data Historical data - Full Non-CMS data (if needed)</td>
</tr>
</tbody>
</table>

4. Press Enter to access the action list, and select Run.
5. After the backup is complete, remove the tape.
6. Label the tape with the date.
7. Reinsert the backup tape.