Avaya^{TM} CMS

R3V11

High Availability Connectivity, Upgrade and Administration

585-215-514
Issue 1.2
October 2002
Compas ID 89409

Notice

Every effort was made to ensure that the information in this book was complete and accurate at the time of printing. However, information is subject to change.

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 working on your company's behalf). Be aware that there may 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 support or assistance, call Technical Service Center Toll Fraud Intervention Hotline at +1 800 643 2353.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or 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 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 to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (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/data privacy, intellectual property, material assets, financial resources, labor costs, and/or 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
- Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products. conforms to the above Directives.

Trademarks

Enterprise, Solaris, Fire, SPARCserver, Sun, SunSwift, Sun Blade, Sun Fire and Ultra are trademarks or registered trademarks of Sun Microsystems, Inc.

INFORMIX is a registered trademark of Informix Software, Inc.

MultiVantage is a trademark of Avaya.

DEFINITY is a registered trademark of Avaya.

All other product names mentioned herein are the trademarks of their respective owners.

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

Select **Support**, then select **Escalation Lists US and International**. This Web site includes telephone numbers for escalation within the United States. For escalation telephone numbers outside the United States, select **Global Escalation List**.

Acknowledgment

This document was written by the CRM Information Development group.

Avaya^{TM} CMS R3V11
High Availability Connectivity, Upgrade and Administration

Contents

Introduction

Connecting HA servers to the switch

Upgrading CMS to the High Availability option

Introduction

The Avaya^{TM} Call Management System (CMS) High Availability (HA) option is a system of hardware and software features designed to reduce potential loss of call center data.

The CMS HA system includes features associated with the Automatic Call Distribution (ACD) feature of Avaya, DEFINITY® or MultiVantage^{TM} switches operating in conjunction with the CMS software application. The CMS HA system consists of the following major features:

- Dual Automatic Call Distribution (ACD) links on the switch
- A paired set of CMS servers, each separately connected to one of the dual ACD links, and through which simultaneous and identical sets of call data are received
- Separate network subnet connections for paired ACD-CMS combinations

HA system redundancy of critical hardware components greatly reduces possible data loss due to single point-of-failure sources. HA also minimizes data loss which might otherwise occur during CMS software upgrades or as a result of software/database corruption problems.

ACD data is simultaneously routed to two CMS servers through paired C-LAN circuit packs or Ethernet ports on the switch over separate TCP/IP over Ethernet subnets.

The CMS servers installed in HA systems are designated as the “primary” and “secondary” servers. The primary server is distinguished from the secondary server by the following differences:

- If the customer has a license for Internet Call Center, it is installed only on the primary server
- Most CMS administration changes are entered only on the primary server. Any changes that are made on the primary server are subsequently transferred to the secondary server by either copying a full maintenance backup or manually making the changes on the secondary server.
- If the customer has the External Call History package, it should be installed on both servers. If the customer has customized report solutions implemented by Avaya, Inc. CRM Professional Services Organization (PSO), External Call History should be active on both servers. Otherwise, it should be active on only the primary server.

Other than the configuration and operational differences listed above, the primary and secondary servers function in a highly similar manner and collect identical data streams through their respective ACD links. Should either server fail or need to be brought down for maintenance, the remaining unit is fully capable of carrying the full CMS activity load without interruption.

Supported switches

The CMS HA option is supported on the following Avaya switches:

- DEFINITY ECS with R8.x, R9.x, R10.x
- DEFINITY servers with MultiVantage Call Center Software
- S8100 Media Server with MultiVantage Call Center Software
- S8300 Media Server with MultiVantage Call Center Software
- S8700 Media Server with MultiVantage Call Center Software

Supported CMS platform combinations

CMS HA is currently supported on the following platform combinations:

- Sun Ultra 5 - Sun Ultra 5
- Sun Enterprise 3000 - Sun Enterprise 3000
- Sun Enterprise 3500 - Sun Enterprise 3000
- Sun Enterprise 3500 - Sun Enterprise 3500
- Sun Fire V880 - Sun Fire V880
- Sun Blade 100 - Sun Ultra 5
- Sun Blade 100 - Sun Blade 100
- Sun Blade 150 - Sun Blade 150
- Sun Blade 150 - Sun Blade 100
- Sun Fire V880 - Sun Enterprise 3500

⚠ **Important:**
Some platforms may require additional hardware or software upgrades in order to be used in a HA configuration.

Recommendations for HA configurations with different Sun platforms

If different Sun platforms must be used for a HA configuration, the more powerful platform should be used as the primary HA server. Some examples would be:

- HA configurations in which Enterprise 3000 and 3500 servers are combined, the 3500 server should be designated as the primary HA server.
- HA configurations in which Enterprise 3500 and Sun Fire V880 servers are combined, the Sun Fire V880 server should be designated as the primary HA server.
- HA configurations in which Ultra 5 Series 1 and 2 and Ultra 5 Series 3 or later servers are combined, the Series 3 or later server should be designated as the primary server.
- HA configurations in which Sun Blade 100 and Ultra 5 servers are combined, the Sun Blade 100 server should be designated as the primary server.
- HA configurations in which Sun Blade 150 and Sun Blade 100 servers are combined, the Sun Blade 150 server should be designated as the primary server.

Required and optional software

A complete set of CMS R3V11 software package CD-ROMs (with the exceptions listed below) is provided for the second server at no additional charge.

For primary and secondary servers deployed in HA systems, the following exceptions to the standard CMS R3V11 software configurations apply:

- X.25 software is not supported as the final connection link between the switch and the HA servers (X.25 can be used to connect remote switches to an on site switch).
- Internet Call Center is never installed on the secondary server.
- If one or more network terminal servers are linked to the primary server and NTS installation is required for the secondary server, then the Bay Networks Annex R10.0B software package provided for the primary server can also be installed on the secondary server.
- If the optional INFORMIX® ISQL software package is installed on the primary server, a second licensed copy of the software must also be purchased by the customer for use on the secondary server.
- If the optional Openlink Open Database Connectivity (ODBC) software package is installed on the primary server, a second licensed copy of the software must also be purchased by the customer for use on the secondary server.

Special upgrade considerations

When an installed CMS HA system is subject to a software upgrade (or when one of the servers is restored to service after a system failure), the alternate server continues to collect data without interruption. Since manual synchronization between the primary and secondary servers is a key maintenance objective for HA systems, CMS upgrades should proceed in a manner that restores synchronization of the servers with the least time and effort, while minimizing data loss as much as possible.

If the CMS server has any custom features, such as Custom Reporting, custom interfaces, LAN printers, token ring, and so forth, PSO must be contacted before the upgrade process is initiated.

For further details of the CMS upgrade process, see Chapter 3, Upgrading CMS to the High Availability option on page 17.

General roles and responsibilities

This document is written for Avaya, Inc. on-site technicians, Technical Service Center (TSC) personnel, software specialists, and customer administrators. The following table lists the major tasks for each switch type, the location of the procedure in the book, and who is responsible for performing each task.

Chapter	Task	Technician	TSC	Software Specialist	Customer
2	Connecting the switch	X			
3	Administering CMS			X	X
4	Administering the switch			X	X
N/A	Troubleshooting switch connections	X	X		

For information about troubleshooting switch connections, see *Avaya Call Management System (CMS) Switch Connections, Administration, and Troubleshooting*, 585-215-876.

Customer-specific roles and responsibilities

Customers are solely responsible for several tasks required to support the CMS HA option. The following table lists tasks for which the customer is solely responsible.

Task
Retention of CMS documentation and software
For those administration changes that are non-transferable via backup tape, revision on each HA server
Nightly full maintenance backups on the primary server
Nightly full maintenance restores on the secondary server
Monthly (or more frequent) CMSADM backups on the primary server
Checking log records to verify success of backup

Reason for reissue

Issue 1.2 adds information about the Sun Blade 150 platform.

Conventions

The following conventions are used in this document:

- Commands you enter from the console are shown in **`bold courier`** font.
- *Italic* text represents variable information.
- Unless specified otherwise, Sun Blade refers to either the Sun Blade 100 computer or the Sun Blade 150 computer.
- Unless specified otherwise, CMS always implies Avaya Call Management System.

Avaya CMS helplines

If a problem arises that requires assistance, use the support information and help lines presented below.

Frequently asked questions (FAQs)

For solutions to common problems, customers and Avaya technicians can access technical support FAQs at:

http://www.avaya.com

Select **Support > Call Center/CRM** and select the product for which you need support. Please check this information before you call in a trouble ticket. It could save you time and money.

Customer support for the United States

Customers can report problems and generate trouble tickets by calling:

1-800-242-2121

The customer is prompted to identify the type of problem (that is, Automatic Call Distribution, hardware, or Avaya CMS) and is then connected to the appropriate service organization.

Technician support for the United States

Avaya technicians can receive help by calling:

1-800-248-1234

Customer and technician support outside the United States

For customer and technician support outside the United States, see the Avaya Web site:

http://www.avaya.com

Select **Support > Escalation Lists US and International**. For escalation telephone numbers outside the United States, select **Global Escalation List**.

Connecting HA servers to the switch

Connecting HA servers to the switch describes connectivity requirements and recommendations specific to CMS High Availability (HA) systems. For more information on supported switches, see, Supported switches on page 6.

The connectivity configurations described in this chapter represent the optimal link setups for HA systems. For detailed connectivity diagrams, see “Connecting the switch link” in *Avaya Call Management System (CMS) Switch Connections, Administration, and Troubleshooting*, 585-215-876.

Basic configuration rules

CMS HA servers do not have to be physically located in the same building, or even in the same city.

CMS HA computers can collect data from up to eight different ACD switches. Mixed ACD links, in which the server is connected to both single ACD links and HA dual links, is not supported. Mixed ACD links could potentially result in significant call data loss and fill system error logs with meaningless data.

Link connections are implemented only by the TCP/IP over Ethernet LAN communications protocol. Connections must run over LAN facilities local to the switch.

Each CMS HA server should be connected to a separate UPS on a separate protected power circuit.

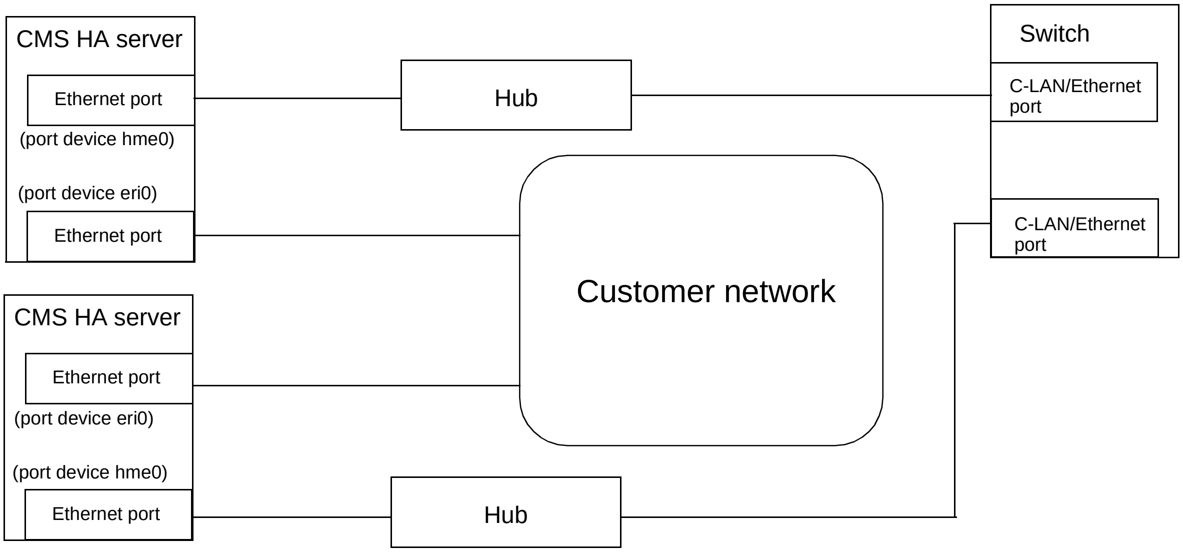
ACD traffic is routed through dual control C-LAN circuit packs or Ethernet ports on the switch. The switch must be administered to enable the dual C-LAN circuit packs or Ethernet ports; for details about the administration of dual ACD links on HA systems, see “Administering the switch link” in *Avaya Call Management System (CMS) Switch Connections, Administration, and Troubleshooting*, 585-215-876.

Ethernet ports on a CMS server

Ideally, a second Ethernet card should be installed on each CMS HA server. If two Ethernet ports are available, the standard provisioning procedure is to use the first (built-in) Ethernet port for connectivity to the customer LAN or public network. The second Ethernet card (Fast-SCSI Buffered Ethernet (FSBE), SunSwift™ Ethernet or SunFast Ethernet) should be dedicated solely to the switch link.

A depiction of an ideal HA system configuration for a single-ACD system is displayed in the following figure.

Local switch configuration diagram



Note:

Existing customer network configurations are likely to require a LAN setup that is different from the idealized configuration shown above, especially when multiple ACDs are connected to the CMS server. For information about alternate LAN configurations, see *Avaya Call Management System (CMS) Switch Connections, Administration, and Troubleshooting*, 585-215-876.

Server switch-over options

The primary purpose of the CMS High Availability offer is to ensure an uninterrupted data stream between the switch and the CMS system on which the data is stored. Some customers may also desire continuous access to their CMS data. Following a major failure event on their primary HA server, customers have the option to switch over to their secondary server for purposes of CMS data monitoring and reporting. A server switch-over should be performed only when the anticipated down time for the primary server is expected to be significant.

Customers must choose between the following switch-over options:

1. **No switch-over**

   Customers who do not require continuous access to their CMS data can choose not to switch over to the secondary server after the primary server experiences a major failure event. When the primary server goes down, uninterrupted collection of call data continues on the secondary server, but the customer is not able to access that data until the primary server is restored.

2. **Manual server switch-overs**

   If uninterrupted access to CMS data is desired, a manual server switch-over must be performed. At a minimum, manual switch-over entails re-administration of CMS Supervisor clients by their individual users in order to redirect the Supervisor clients from the primary to secondary server.

   Depending on the nature of the customer network, additional measures may be required, such as re-administration or addition of NTS servers, physical reconnection of peripheral devices, and so forth. Customers considering the manual switch-over option should consult with their TSO and/or PSO representatives in order to discuss logistical issues associated with manual server switch-overs.

Upgrading CMS to the High Availability option

Upgrading CMS to the High Availability option describes Avaya^{TM} Call Management System (CMS) upgrade procedures used to combine a new CMS server with an existing CMS system in order to create a CMS High Availability (HA) system.

The CMS servers used in an HA system must have the same CMS version and base load number. If the original server has a different CMS version from the new server being added to the system, upgrade of the original server must be performed by means of an Avaya CMS Upgrade Express (CUE) upgrade. In many cases, the new HA systems will consist of an existing CMS installation combined with a newly purchased CMS server. The two CMS servers incorporated into the system are referred to as follows:

- Original server – the CMS server that is already installed on site
- New HA server – the server purchased by the customer to enable the HA option

CMS software combinations

One of the following CMS software combinations will apply for your upgrade:

- The CMS servers have the same CMS version and base load.
- The CMS servers have the same CMS version but the base load is different.
- The original server has an earlier version of CMS than the version installed on the new HA server

Note:

If a hardware upgrade is required for your platform configuration, you may be required to perform a CUE upgrade.

Things to consider if the servers have the same CMS version

When an original server is already installed with the correct CMS version, logistics associated with creation of a new HA system are greatly simplified because:

- The switch can be administered for the correct CMS version and the dual ACD links prior to the arrival of the new HA server on site. The unused switch link is busied out until the new HA server is installed.
- The original server either does not require a software upgrade or needs only a base load upgrade to match the installation on the new HA server.

Achievement of a synchronized system requires minimal or no software installation, followed by one or two maintenance backups and restores between the two servers. The servers are never truly synchronized because of operational differences between the primary and secondary servers.

When an original server is already installed with the correct CMS version, logistics associated with creation of a new HA system are greatly simplified.

Things to consider if the servers have different CMS versions

If the original server is installed with an earlier version of the CMS software, then the HA upgrade process entails a specific sequence of installation and administration activities in addition to various maintenance backups, data migrations, and data restores. These activities must be executed in an ordered sequence intended to minimize system downtime and overall provisioning effort. The procedures required to perform an HA upgrade under this scenario are presented in the following sections.

About the HA upgrade process

About the HA upgrade process presents an overview of the steps required to upgrade the CMS version of a HA server. This process describes only that upgrade scenario in which a full CMS version upgrade is required. For more information about the base load upgrade process, see *Avaya CMS R3V11 High Availability User Guide*, 585-215-714.

Prerequisites

Before you begin the HA upgrade process, verify that you have at least three tapes available to backup the system.

Steps to perform 24 hours before the upgrade

You must perform the following steps approximately 24 hours before the upgrade:

1. Upgrade the switches to Release 8.1 or later and administer the switches to run with the current version of CMS installed on the original server.

   Example:

   If the current version of CMS installed on the system is R3V9, then upgrade the switch and administer it for a R3V9 system.

2. Verify that the tape drive on the original server is compatible with the tape drive on the new HA server because backup tapes will be exchanged between the two servers. For more information, see Verifying the tape drive on the server currently in service on page 23.

   Note:

   > If replacement of the tape drive on the original server is required, Provisioning will dispatch a Sun technician. If the call center operates on a 24/7 basis, this activity will incur some loss of CMS data.

3. Avaya services and the customer must coordinate to:

   a. Determine which CMS server will be designated as the primary server and which will be designated as the secondary server. For more information, see Supported CMS platform combinations on page 6.

   b. Establish a cut-off time on the day of the HA upgrade. After the designated cut-off time, CMS users will not be able to make changes to the system administration until the upgrade is complete.

4. Perform a CMSADM backup and a CMS full maintenance backup on the original server. For more information, see Performing a CMSADM backup on page 25 and Performing a full maintenance backup on page 27.

Steps to perform the day of the upgrade

You must perform the following steps the day of the upgrade:

1. On the day of the upgrade, the Avaya technician arrives on site and performs a backup of system and ACD-specific administration data on the original server.

   ⚠ **Important:**
   At this point in the upgrade process, CMS users must not attempt to make administrative changes on the system until the HA upgrade is completed.

2. The technician installs and configures the new HA server. The technician puts CMS into single user mode and the CMSADM backup tape (created in Step 4 of Steps to perform 24 hours before the upgrade on page 19) is used to migrate the system administration data and agent/call center administration data onto the new HA server.
3. After the most recent intrahour interval archive completes on the original server, busy out all ACD links at their respective switches and re-administer them for CMS R3V11 and dual ACD links. When the switches are re-administered, release the busy out for the links.
4. As soon as the switch is re-administered and the ACD links for the new HA server come up, verify that CMS data collection on the new HA server is active for all ACDs.
5. Perform an incremental maintenance backup on the original server (historical data only), and then turn off the system. Do all other required pre-upgrade procedures which are necessary prior to starting the Avaya CMS Upgrade Express (CUE) upgrade. Refer to the platform-specific instruction booklet included in the CUE upgrade kit. Then perform the rest of the CUE upgrade.
6. After the CUE upgrade is complete and the new CMS software has been set up, restart CMS data collection on the original server. Verify that data is collected from all ACDs.
7. Migrate the CMS historical data from the incremental maintenance backup (Step 5) to the new HA server. When the migration completes, replace the incremental tape with the original full maintenance tape (created in Step 4 of Steps to perform 24 hours before the upgrade on page 19) and migrate all of the remaining historical data to the new HA server.
8. Use the CMS system administration and ACD-specific administration data backup tape (Step 1) to migrate that data back onto the newly upgraded original CMS server.
9. Run a full maintenance backup on the new HA server. For more information, see Performing a full maintenance backup on page 27.
10. Restore the historical data from the full maintenance backup tape (created in Step 9) onto the original server.

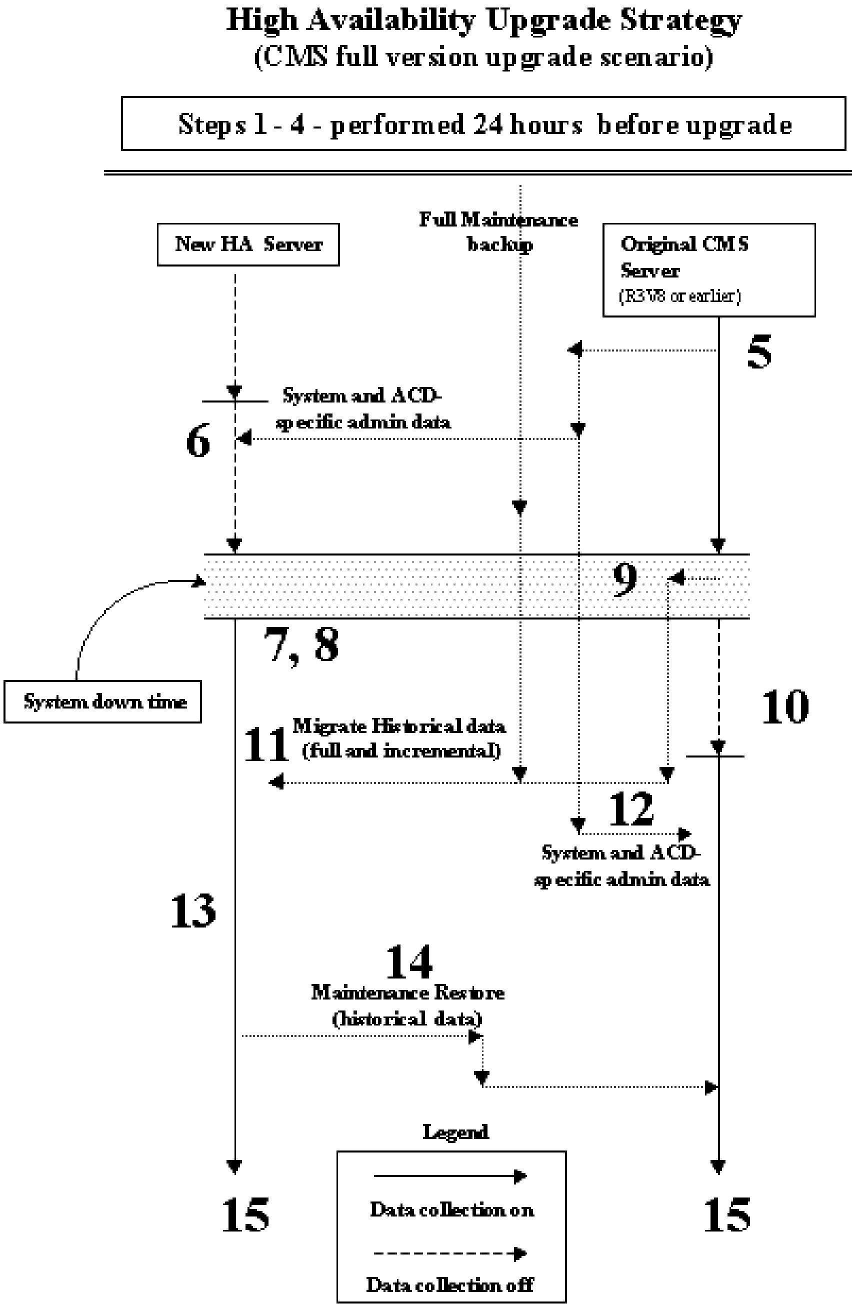
    The two servers now share the same initial set of administrative data. *CMS users can now resume or begin making administrative changes to whichever CMS system is designated as the primary server.*

11. Run CMSADM backups on both servers.

The CMS HA upgrade process is now complete. Customers should initiate a regular maintenance schedule.

For more information, see the Schematic depiction of the HA Upgrade procedure when a full CMS version upgrade is required: on page 22 and *Avaya CMS R3V11 High Availability User Guide*, 585-215-714.

Schematic depiction of the HA Upgrade procedure when a full CMS version upgrade is required:


High Availability Upgrade Strategy
(CMS full version upgrade scenario)
Steps 1 - 4 - performed 24 hours before upgrade
New HA Server
Full Maintenance backup
Original CMS Server
(R3V8 or earlier)
5
System and ACD-specific admin data
6
9
7, 8
System down time
10
11
Migrate Historical data (full and incremental)
12
System and ACD-specific admin data
13
14
Maintenance Restore (historical data)
Legend
Data collection on
Data collection off
15
15

Verifying the tape drive on the server currently in service

New systems are currently offered with the DDS-4 tape drive. The Mammoth tape drive and SLR5 tape drive are no longer shipped with new systems but are shown here to support existing systems. If a new system with a DDS-4 tape drive is combined with an existing system with an older model tape drive, you will need to replace the older model tape drive with a DDS-4 tape drive.

The tape drive replacement, which is performed by a Sun technician, must be completed before the HA upgrade process is initiated.

⚠ **WARNING:**

After the original tape drive on an Enterprise 3000 has been replaced, you must discard any tapes which were in use with the old drive. *Re-use of old tapes on the replacement drive will damage the tape device.*

Platform considerations

This procedure is required only for HA systems when:

- An E3000 server currently in service and equipped with a 14-GB tape drive, is combined with a new E3500 platform equipped with a Mammoth drive
- An E3500 server currently in service and equipped with a Mammoth tape drive, is combined with a new V880 platform equipped with a DDS-4 drive
- An Ultra 5 server currently in service and equipped with an SLR5 tape drive, is combined with a new Ultra 5 equipped with a DDS-4 drive
- An Ultra 5 server, currently in service and equipped with an SLR5 tape drive, is combined with a new Sun Blade 100 equipped with a DDS-4 drive

Verifying the Mammoth tape drive

The Mammoth tape drive is no longer shipped with new systems, but is shown here to support existing systems. If replacement of the tape device is required for an existing Enterprise 3000 system prior to beginning an upgrade to the High Availability option, use this procedure to confirm that the old tape drive is replaced by a new Mammoth drive:

1. Insert an 8mm 170m AME tape cartridge in the tape drive.

2. Enter:

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

   If the drive has been replaced, the system responds:

```
Mammoth EXB-8900 8mm Helical Scan tape drive:
   sense key(0x0)= No Additional Sense   residual= 0   retries= 0
   file no= 0   block no= 0
```

Verifying the DDS-4 tape drive

If replacement of the tape device is required for an existing system prior to beginning an upgrade to the High Availability option, use this procedure to confirm that the old tape drive has been replaced by a new DDS-4 drive:

1. Insert a 150mm 20GB DAT cartridge in the tape drive.
2. Enter:

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

   If the drive has been replaced, the system responds:

```
Vendor ’HP   ’ Product ’C5683A   ’ tape drive:

sense key(0x0)= No Additional Sense
residual= 0  retries= 0  file no= 0  block no= 0
```

Performing a CMSADM backup

A CMSADM file system backup saves all system files (excluding CMS call data) and is used to restore the system in the event of an upgrade failure. A CMSADM backup must be performed within 24 hours of the start of the HA upgrade process. CMSADM backups must also be performed on both servers immediately after the completion of the HA upgrade.

The CMSADM file system backup includes the following:

- Solaris system files and programs
- CMS programs
- Non-CMS customer data placed on the computer

Procedure

To perform a CMSADM backup:

1. Log in as **root** and enter:

   `cmsadm`

   The **Avaya Call Management System Administration Menu** is displayed.

2. Enter the number associated with the `backup` option.
3. Depending on the configuration of your system, go to a or b, below.

   a. If only one tape drive is available on the system, the program responds:

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

   b. If more than one tape drive is available for use by the system, the program will display output similar to the following example:

   ```
   Select the tape drive:
     1) Exabyte EXB-8900 8mm Helical Scan tape drive: /dev/rmt/0
     2) Exabyte EXB-8500 8mm Helical Scan tape drive: /dev/rmt/1
   Enter choice (1-2):
   ```

4. Enter a tape drive selection from the displayed list. The program displays:

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

Note:

If only one tape drive is available, the output shown above is not displayed.

5. Press **Enter**.

   The backup process begins. If more than one tape is required, the program displays the following message:

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

   If you see the message displayed above, insert the next tape and allow it to rewind. When it is properly positioned, press **Enter**.

6. When the backup is complete, the program response varies according to the number of tapes used for the backup:

   - If the number of tapes required is one, the system responds:

```
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 (r3vXxx.x)
```

   - If the number of tapes required is more than one, the system responds:

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

     If you see the second message, insert the first tape used in the backup and press **Enter**. Wait for the tape drive light-emitting diode (LED) to stop blinking before you remove the tape.

     When prompted, repeat this process for any additional tapes generated by the backup process. When the final tape is verified, the program displays the output shown above in Step 6.

7. Save the tapes until a restore is performed on the system.

   CAUTION:

   Label all tapes with the tape number and the date of the backup. Set the tape write-protect switch to read-only.

Performing a full maintenance backup

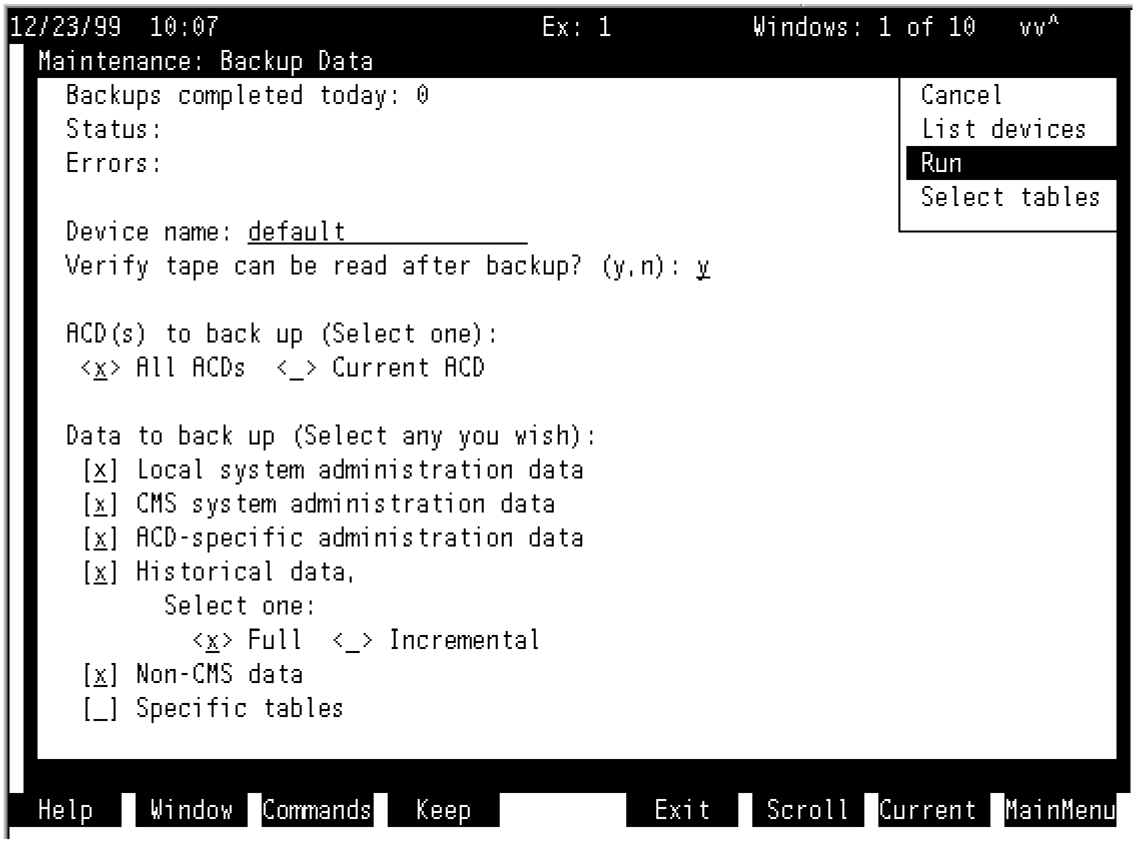
Before an existing CMS server is incorporated into a new HA system, the customer must perform a CMS full maintenance backup within 24 hours of starting the HA upgrade process.

Procedure

To perform a full maintenance backup:

1. Log in as a CMS user and select **Maintenance** > **Back Up Data** option from the main menu.

   The **Back Up Data** window is displayed.



```
12/23/99  10:07                     Ex: 1        Windows: 1 of 10   vv^
 Maintenance: Backup Data
   Backups completed today: 0
   Status:
   Errors:

   Device name: default
   Verify tape can be read after backup? (y,n): y

   ACD(s) to back up (Select one):
    <x> All ACDs  <_> Current ACD

   Data to back up (Select any you wish):
    [x] Local system administration data
    [x] CMS system administration data
    [x] ACD-specific administration data
    [x] Historical data,
          Select one:
            <x> Full  <_> Incremental
    [x] Non-CMS data
    [_] Specific tables
```

2. To accept the default backup options, press **Enter** to activate the action list in the upper right corner of the window.
3. Select the `Run` option and press **Enter**.

Performing a maintenance backup of only the administration data

When the CMS technician arrives on site, the technician performs an initial maintenance backup on the original server. This backup should include only CMS system administration data, ACD-specific administration data, and non-CMS data.

Note:

Once this backup is started, CMS users must not make any new administrative changes to the system until the upgrade process is finished.

Procedure

To perform a maintenance backup of the administration data:

1. From the CMS main menu, select **Maintenance** > **Back Up Data**.

   The **Back Up Data** window is displayed.

2. Select the following data backup options:

   - ACDs to backup — all ACDs
   - CMS system administration data
   - ACD-specific administration data
   - Non-CMS data

   Exclude **Historical data** from this backup

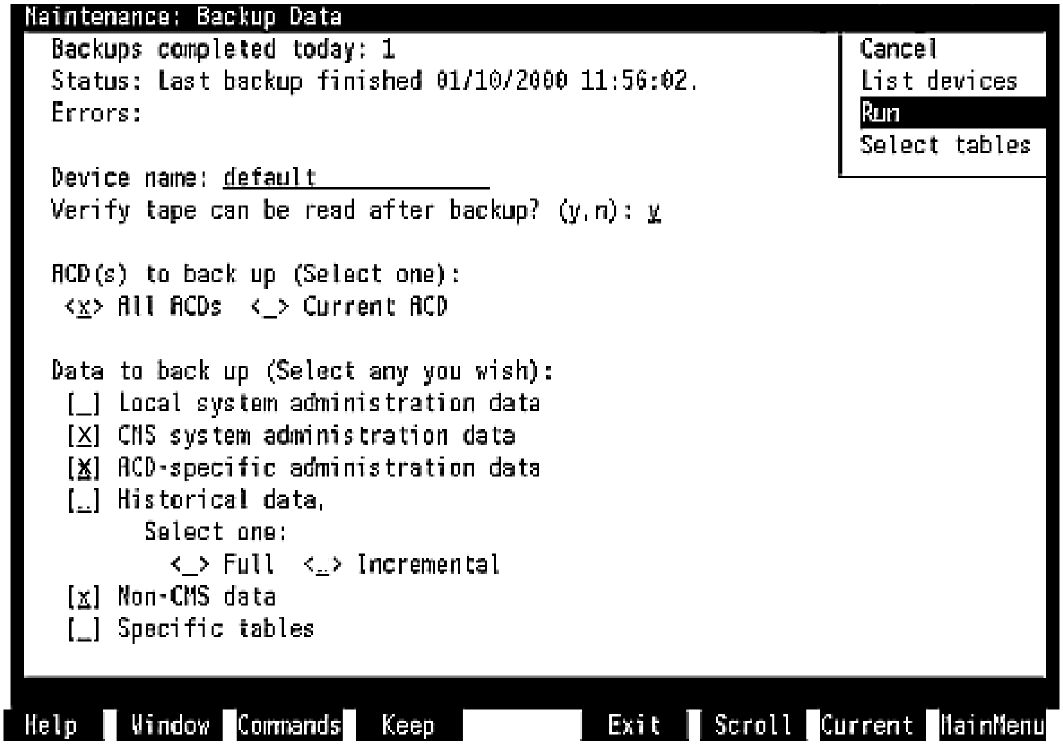
3. Press **Enter** to move the active cursor to the action list in the upper right corner of the window.

4. Select **Run** and press **Enter**.

⚠ **CAUTION:**

> The HA upgrade entails the use of multiple backup tapes. Be careful to label these tapes appropriately; use of the wrong tape during a migration or restore may result in failure to achieve an initial state of synchronization between the two HA servers.

The correct backup option selections are shown in the following example:



```
Backups completed today: 1
Status: Last backup finished 01/10/2000 11:56:02.
Errors:

Device name: default
Verify tape can be read after backup? (y,n): y

ACD(s) to back up (Select one):
 <x> All ACDs  <_> Current ACD

Data to back up (Select any you wish):
 [_] Local system administration data
 [X] CMS system administration data
 [X] ACD-specific administration data
 [_] Historical data.
       Select one:
         <_> Full  <_> Incremental
 [x] Non-CMS data
 [_] Specific tables
```

After you have selected the appropriate options for the backup, press **Enter** to activate the action list in the upper right corner of the window. Move the cursor to the **Run** option and press **Enter** to start the backup.

5. To verify that the backup completed without errors:

   a. Open a terminal window and enter:

      `cms/bin/br_check`

      The system responds:

```
Enter device type [q for qtape, f for floppy]:
```

b. Enter: **q**

The system responds:

```
Enter device path:
```

c. Enter the device path for the tape drive.

Example:

`/dev/rmt/0c`

The system displays a list of ACD(s) backed up on the volume and prompts:

```
Enter l to list the tables or v to also verify the volume:
```

d. Enter: **`l`**

The system displays a list of the database tables included on the backup.

Setting up CMS on an HA server

Setting up CMS on an HA server refers to procedures that apply to both the new HA server and the original server. The original server and the new HA server must have the same CMS version and base load.

⚠ **Important:**
Most of the procedures listed in this section refer to another document. Each of the procedures should be reviewed for HA-specific information before you use the associated procedures from another document.

TSC personnel verify authorizations, set up data storage parameters, and set up the CMS application remotely. On-site technicians should call the TSC to coordinate this process.

Prerequisites

The TSC should verify that:

- A copy of *Avaya CMS R3V11 Software Installation, Maintenance and Troubleshooting Guide*, 585-215-115 is available for reference
- A copy of *Avaya CMS Switch Connections Administration and Troubleshooting*, 585-215-876 is available for reference
- A copy of *Avaya CMS Terminals Printers and Modems*, 585-215-874 is available for reference
- The console is connected to the CMS computer
- The CMS computer is connected to the TSC Remote Maintenance Center (remote console).
- Additional terminals and printers are connected to the NTS ports.
- The link between the CMS computer is connected to the switch.

  ⚠ **Important:**
  If the hardware link or the Automatic Call Distribution (ACD) feature and CMS are not properly administered, the CMS software cannot communicate with the switch. For switch administration procedures, see “Administering the switch link” in *Avaya CMS Switch Connections Administration and Troubleshooting*.

- The NTS and the CMS computer are connected to the network hub unit. For more information, see *Avaya CMS Terminals Printers and Modems*.

Contents

Setting up CMS on an HA server contains the following procedures:

Setting CMS authorizations

Before setting up CMS, TSC personnel need to set authorizations for CMS features purchased by the customer. Authorizations apply to all administered ACDs. For the procedure used to set up CMS authorizations, see “Setting up CMS authorizations” in the CMS software installation, maintenance and troubleshooting guide.

Setting up data storage parameters

TSC personnel modify specific data storage parameters on the CMS computer so that the CMS application can operate properly. The **storage.def** file contains these data storage parameters, which are installed with a set of standard default values.

Review the default data storage values for each authorized ACD. The default values are found on the line immediately below each storage parameter, and many of them can be edited to meet the needs of individual customers. Use the values determined by the Account Executive, System Consultant, or Design Center based on the customer configuration.

> ⚠ **Important:**
> For a new HA system being added to an existing CMS installation, data storage values should be identical to the values installed on the original server at the customer site.

For the procedure used to set up data storage parameters, see “Setting up CMS data storage parameters” in the CMS software installation, maintenance and troubleshooting guide.

Setting up a LAN for switch connections

Setting up a LAN for switch connections contains information about setting up a LAN connection between the CMS computer and one or more HA-enabled switches. This type of connection is used only with switch Release 8.1 or later. The LAN connections described herein are based on the configuration recommended for HA systems, which includes two Ethernet ports for each server and which assumes that private LAN subnets are used for the switch-to-server connections.

To set up a LAN connection to an HA-enabled switch, you must coordinate the administration done on the CMS computer with the administration done on the switch and, if required, within the customer’s own data network.

⚠ **Important:**

Before you begin this procedure:

- Verify that you are logged in as root user.
- CMS must be turned off.
- All file systems must be mounted.

For the procedure used to set up data storage parameters, see “Setting up LAN connections” in the CMS software installation, maintenance and troubleshooting guide.

Setting Up the CMS application

The CMS application allows you to measure call center performance.

⚠ **Important:**

Before you begin this procedure:

- Verify that you are logged in as root user.
- CMS must be turned off.
- All file systems must be mounted.

For the procedure used to set up data storage parameters, see “Setting up the CMS application” in the CMS software installation, maintenance and troubleshooting guide.

Installing feature packages

These procedures are used to install the following feature packages:

- Forecasting
- External Call History Interface (ECHI).

Customers can install the Forecasting or ECHI feature packages if they have been authorized during CMS setup. For feature package installation procedures, see “Installing feature packages” in the CMS software installation, maintenance and troubleshooting guide.

Considerations for running ECHI in the HA environment

When a CMS customer is using ECHI in an HA environment, the ECHI software should be installed on both the primary and secondary servers. The recommended practice for running ECHI on the HA servers depends on the customer-specific factors:

- If the customer is using ECHI in support of customized reporting features implemented by the Avaya Professional Services Organization (PSO), ECHI should be active on both the primary and secondary features.
- If the customer is not using ECHI in support of customized reporting features implemented by PSO, the ECHI software should be active on the primary server and turned off on the secondary server.

Setting up the remote console

Redirecting the remote console port allows the TSC to dial in and perform remote maintenance. Remote access is required for both the primary and secondary servers. For procedures used to administer and test the remote console port on the back of the CMS computer, see “Setting up the remote console” and “Redirecting the remote console port to the modem” in the CMS software installation, maintenance and troubleshooting guide.

Setting up the Alarm Origination Manager

The setup of the AOM config files is usually performed by the database group when a new system is administered for AOM. A product ID number must be obtained from the CMS database administration group. CMS technical support personnel contact the database group at 800-248-1111, ext. 07425 and provide them with the customer IL number.

If the AOM system administration information for the server is already established by the database group, and a product ID is available, the config file setup can be performed manually by provisioning personnel. For a description of the AOM config file set up, see “Setting up the alarm origination manager” in the CMS software installation, maintenance and troubleshooting guide.

Setting up the NTS

For information about setting up the NTS, see “Setting up the NTS” in *Avaya CMS Terminals, Printers, and Modems*.

Creating an alternate boot device for mirrored systems

This procedure creates an alternate boot device. This procedure is required only for Enterprise 3000, Enterprise 3500, Sun Fire V880 or Sun Blade platforms configured as mirrored systems. For a description of the procedure used to create the alternate boot device, see “Creating an Alternate Boot Device for Mirrored Systems” in the CMS software installation, maintenance and troubleshooting guide.

Migrating CMS system administration data to the new server

Migrating CMS system administration data to the new server uses the maintenance backup tape which was created during the procedure described in Performing a maintenance backup of only the administration data on page 28. The backup was created on the original server in order to migrate administration data onto the new HA server.

The immediate objective is to bring the new HA server to an operational state as quickly as possible. CMS Historical data is not migrated onto the new HA server until later in the upgrade process.

⚠ **CAUTION:**

The backup used in this procedure includes only CMS system administration data, ACD-specific administration data, and non-CMS data. *Do not use the full maintenance backup tape created in* Performing a full maintenance backup on page 27 *for this migration.*

Procedure

For all versions of CMS Release 3, migrate the system administration data via the **R3 Migrate Data** window.

⚠ **CAUTION:**

Attempting to migrate system administration data more than once may cause catastrophic errors from which recovery is difficult. Before a re-migration of system administration data can be performed, you must turn off CMS and perform a second setup of the CMS software.

To migrate CMS system administration data to the new server:

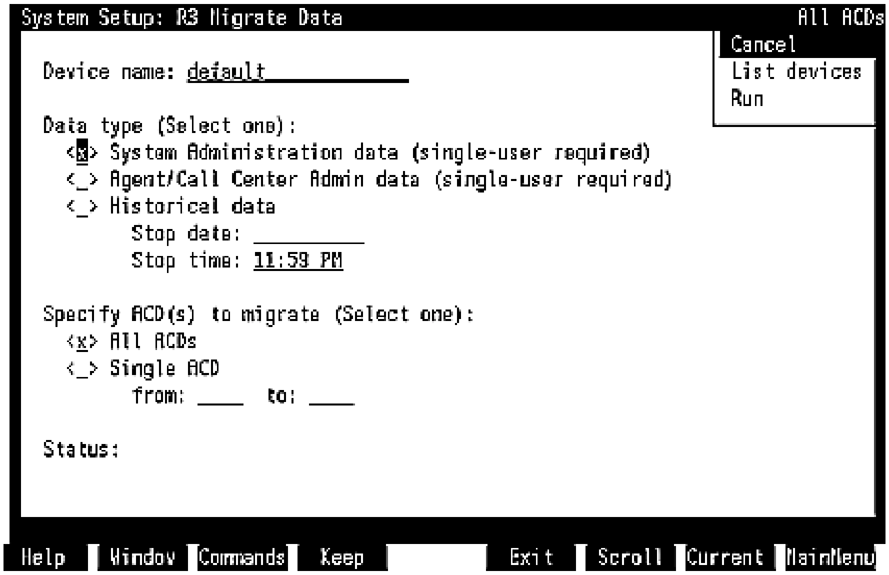
1. Log into CMS.

   The CMS main menu is displayed.

2. From the CMS main menu, select **System Setup** > **CMS State**
3. Select **Single User Mode**.
4. Insert the backup tape that contains the latest version of the administration data into the tape drive on the new HA server.
5. Select **System Setup** > **R3 Migrate Data** from the CMS main menu.

   The **System Setup: R3 Migrate Data** window is displayed.

6. Specify **System Administration data** as the migration data types, and specify **All ACDs** for migration, as shown in the following example:



```
System Setup: R3 Migrate Data                                    All ACDs

  Device name: default___________

  Data type (Select one):
    <x> System Administration data (single-user required)
    <_> Agent/Call Center Admin data (single-user required)
    <_> Historical data
          Stop date: _________
          Stop time: 11:59 PM

  Specify ACD(s) to migrate (Select one):
    <x> All ACDs
    <_> Single ACD
          from: ____   to: ____

  Status:
```

7. Press **Enter** to access the action list in the top right corner of the window.
8. Select **Run** and press **Enter**.

   The **Status:** field reports the progress of the migration, and when the migration ends, indicates success or failure.
9. Repeat the procedure, this time selecting **Agent/Call Center Admin data** as the data type to be migrated.

   Again, the **Status:** field reports the progress of the migration, and when the migration ends, indicates success or failure.

   ⚠ **Important:**

   Printer administration must be done on the new HA server before Step 10 can be performed.
10. To print out the customer migration log, enter:

    ```
    lp /cms/migrate/r3mig.log
    ```

For help interpreting the log and its messages, U.S. customers can contact CMS technical support at 1-800-242-2121; international customers should contact their Avaya distributors or customer representatives.

The services migration log is located at **/cms/maint/r3mig/mig.log**

Checking the archive interval

When you are ready to upgrade the CMS software on the original server, wait for the current archive interval to complete before busying out the link. This avoids unnecessary loss of call data.

To check the archive interval status:

1. Log in as a CMS user and select **Maintenance** from the CMS Main Menu.

   The **Maintenance** options window is displayed.

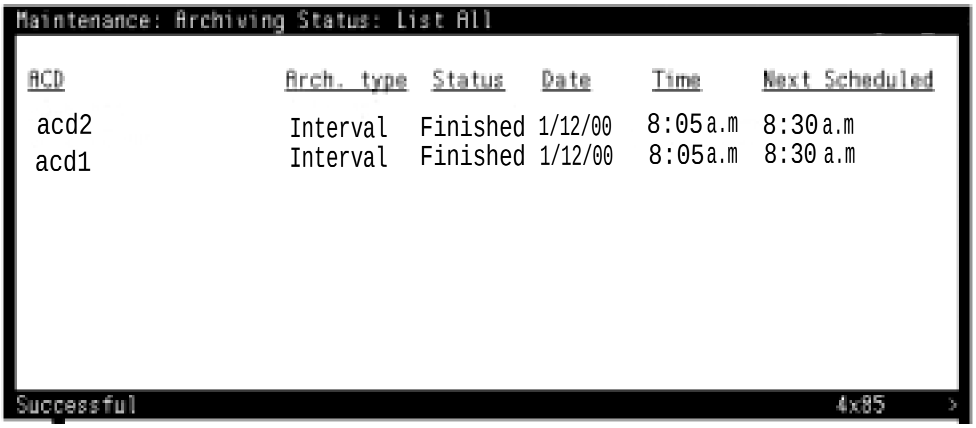
2. Cursor down to the **Archiving Status** option and press **Enter**.

   The **Maintenance: Archiving Status** window is displayed.

3. Cursor down to the **Archiving type** list and use the spacebar to deselect the **Daily, Weekly** and **Monthly** options.

4. Press **Enter** to activate the action box in the top right corner of the window; press **Enter** again to select the **List all** option.

   The **Maintenance: Archiving Status: List all** window is displayed.



```
Maintenance: Archiving Status: List All

ACD                        Arch. type  Status    Date     Time     Next Scheduled
acd2                       Interval    Finished  1/12/00  8:05a.m  8:30a.m
acd1                       Interval    Finished  1/12/00  8:05a.m  8:30a.m

Successful                                                        4x85
```

5. Look at the figures in the **Time** column. If the elapsed time since the last archive completion is not more than a few minutes, proceed with the link busy out. If more than a few minutes has elapsed since the last archive completion, wait for the next archive interval to complete before busying out the link.

Administering the switch

After links to the original server are busied out at the switch, the switch is re-administered for the new CMS version and the HA dual C-LAN or Ethernet port option.

For details of switch administration for HA systems, see “Administering the switch link” in *Avaya CMS Switch Connections Administration and Troubleshooting*, 585-215-876.

After you have re-administered the switch, bring up the links and start data collection on the new HA server. At this point in the HA upgrade process, both CMS systems are offline and call data is not collected. Therefore, you should complete administration of the switch for the new CMS version and HA dual links, followed by startup of data collection on the new HA server, as quickly as possible.

Note:

Be sure to verify that data collection is active on all ACD links before you begin the next procedure.

The services migration log is in **/cms/maint/r3mig/mig.log** The log may contain information not intended for the customer.

Performing an incremental maintenance backup

Perform an incremental maintenance backup (historical data only) on the original server. Begin the server upgrade immediately after the backup is complete.

Procedure

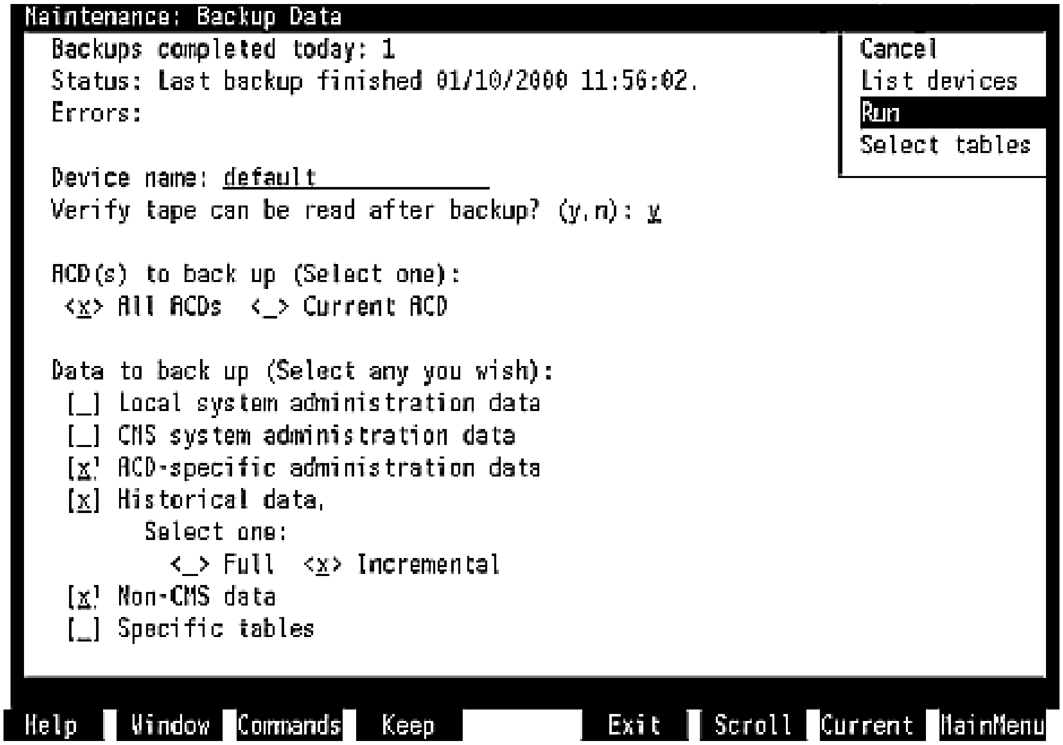
To perform an incremental maintenance backup:

1. From the CMS main menu, select the **Maintenance** > **Back Up Data**.

   The Back Up Data window is displayed.

2. Select only the **Historical data** > **incremental** data type to be copied onto the backup.

   The correct backup option selections are shown in the following example:



```
Maintenance: Backup Data
  Backups completed today: 1
  Status: Last backup finished 01/10/2000 11:56:02.
  Errors:

  Device name: default
  Verify tape can be read after backup? (y,n): y

  ACD(s) to back up (Select one):
   <x> All ACDs  <_> Current ACD

  Data to back up (Select any you wish):
   [_] Local system administration data
   [_] CMS system administration data
   [x] ACD-specific administration data
   [x] Historical data,
         Select one:
           <_> Full  <x> Incremental
   [x] Non-CMS data
   [_] Specific tables
```

3. After you have selected the appropriate options for the backup, press **Enter** to activate the action list in the upper right corner of the window. Select the **Run** option and press **Enter** to start the backup.

Upgrade the original CMS server

As soon as the incremental backup (for more information, see Performing an incremental maintenance backup on page 40) is successfully completed on the original server, the original server can be powered down, the CUE upgrade is performed, and all necessary software authorization, setup, and configuration steps are also performed. For details, see Setting up CMS on an HA server on page 31.

By the time the upgrade of the original server is complete and data collection is turned on, the new HA server should be fully operational.

The final steps in the HA upgrade process, which includes two separate data migrations, a final full maintenance backup and restore, and the creation of CMSADM backups for each of the HA servers, are described in the following procedures.

Migrating CMS historical data to the new HA server

After the switch is re-administered for the upgraded CMS version, the HA dual C-LAN option is enabled and CMS data collection is started on the new HA server, CMS historical data can be migrated to the new HA server. This procedure migrates CMS historical data from the second incremental maintenance backup (see Performing an incremental maintenance backup on page 40) to the new HA server.

Procedure

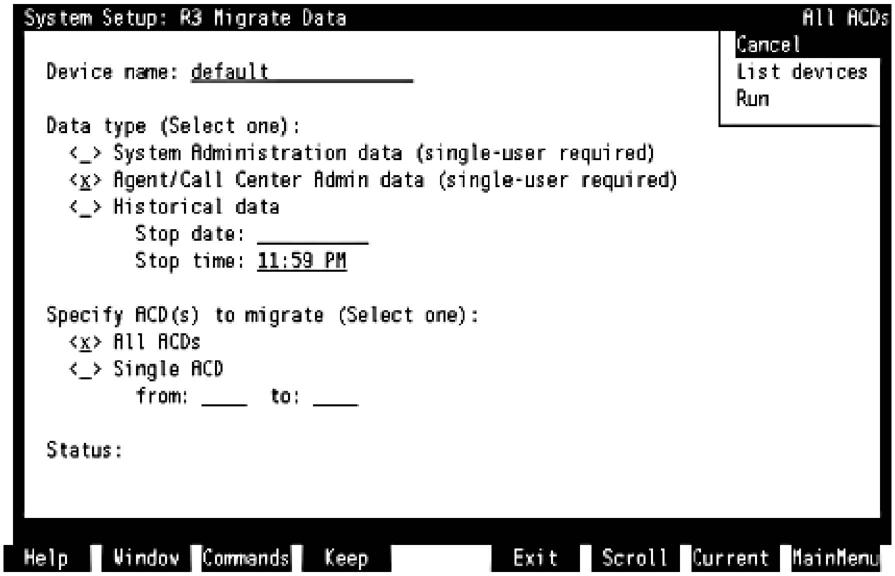
To migrate CMS historical data to the new HA server:

⚠ **WARNING:**

Attempting to migrate CMS data more than once may cause catastrophic errors from which recovery is difficult. Before a re-migration of data can be performed, CMS must be turned off and a second setup of the CMS software must be performed.

1. Insert the incremental maintenance backup tape that contains incremental historical data into the tape drive on the new HA server.
2. Select **System Setup** > **R3 Migrate Data** from the CMS main menu.

   The **System Setup: R3 Migrate Data** window is displayed.
3. Select **Historical data** as the data type, and **specify All ACDs** for migration, as shown in the following example:



```
System Setup: R3 Migrate Data                                    All ACDs

  Device name: default___________

  Data type (Select one):
    <_> System Administration data (single-user required)
    <x> Agent/Call Center Admin data (single-user required)
    <_> Historical data
          Stop date: ________
          Stop time: 11:59 PM

  Specify ACD(s) to migrate (Select one):
    <x> All ACDs
    <_> Single ACD
          from: ___   to: ___

  Status:
```

4. Press **Enter** to activate the action list in the top right corner of the window.
5. Select **Run** and press **Enter**.
6. The **Status:** field reports the progress of the migration, and when the migration ends, indicates success or failure.
7. When the migration is finished, remove the incremental tape from the drive and insert the original full maintenance backup tape (see Performing a full maintenance backup on page 27) and repeat Steps 2 through 6.

   Note:

   Printer administration must be done on the new HA server before Step 8 can be performed.

8. To print out the customer migration log, enter:

   ```
   lp /cms/migrate/r3mig.log
   ```

   For help interpreting the log and its messages, U.S. customers can contact CMS technical support at 1-800-242-2121; non U.S. customers should contact their Avaya distributors or customer representatives.

   The services migration log is found in **/cms/maint/r3mig/mig.log**

Migrating administration data back to the original server

After the original server is upgraded to the same CMS version and base load as the new HA server, the original administration data, which was copied to tape in the first maintenance backup (Performing a maintenance backup of only the administration data on page 28) is migrated back onto the system. After this procedure is performed, the two servers should share identical sets of administration data.

⚠ **WARNING:**
Attempting to migrate CMS data more than once may cause catastrophic errors from which recovery is difficult. Before a re-migration of data can be performed, you must turn off CMS and a second setup of the CMS software must be performed.

Migrate the administration data

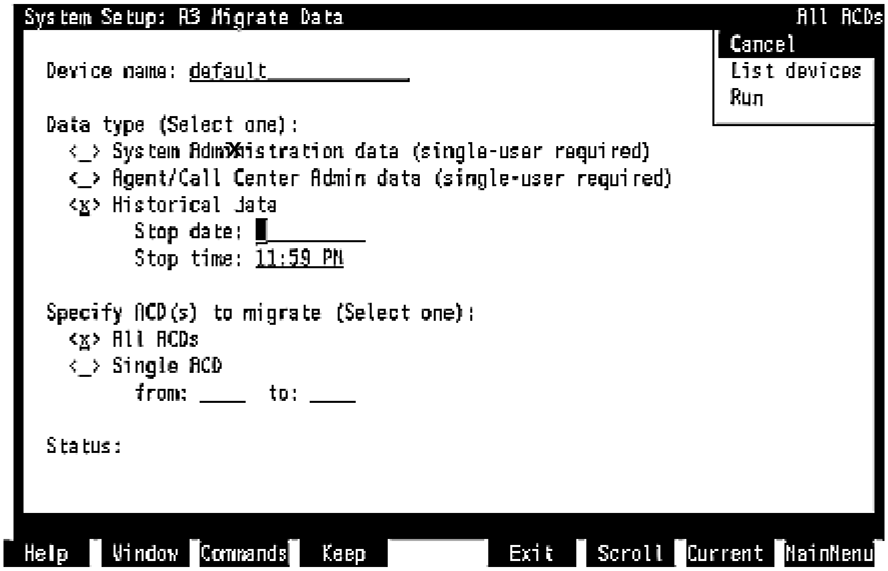
To migrate the administration data:

1. Insert the initial maintenance backup tape back into the tape drive of the original server.
2. Log in as a CMS user.

   The CMS main menu is displayed.
3. Select **System Setup** > **CMS State** from the CMS main menu and select **Single User Mode**.
4. Select **System Setup** > **R3 Migrate Data** from the CMS main menu.

   The **System Setup: R3 Migrate Data** window is displayed.

5. Select **CMS administration data** and **Agent/Call center admin data** as data types and specify **All ACDs** for migration, as shown in the following example:



```
System Setup: R3 Migrate Data                                  All ACDs

  Device name: default____________

  Data type (Select one):
    <_> System AdmXnistration data (single-user required)
    <_> Agent/Call Center Admin data (single-user required)
    <x> Historical Jata
          Stop date: █________
          Stop time: 11:59 PM

  Specify ACD(s) to migrate (Select one):
    <x> All ACDs
    <_> Single ACD
          from: ____  to: ____

  Status:
```

6. After you verify that the correct options are selected, press **Enter** to activate the action list in the top right corner of the window.
7. Select **Run** and press **Enter**.

   The **Status:** field reports the progress of the migration, and when the migration ends, indicates success or failure.
8. Select **System Setup** > **CMS State** from the CMS main menu
9. Select **Multi User Mode**.
10. Verify that data collection is on for all ACD links.
11. To print out the customer migration log, enter:

    ```
    lp /cms/migrate/r3mig.log
    ```

    For help interpreting the log, U.S. customers can contact CMS technical support at 1-800-242-2121; international customers should contact their Avaya distributors or customer representatives.

    The services migration log is stored in **/cms/maint/r3mig/mig.log**

Performing a new full maintenance backup and restore

These procedures create a full maintenance backup on the new HA server. The backup is then used to restore CMS historical data back onto the original server.

Performing the full maintenance backup on the new HA server

The required full maintenance backup copies all system data to tape. For details, see Performing a full maintenance backup on page 27.

Note:

Assuming that the new HA server is used as the HA primary server, this backup represents the first tape to be archived for the new HA system. The other backup tapes used during the provisioning process may now be reused for nightly maintenance backups.

Restoring historical data to the original server

This procedure copies historical data from the full maintenance backup.

Procedure

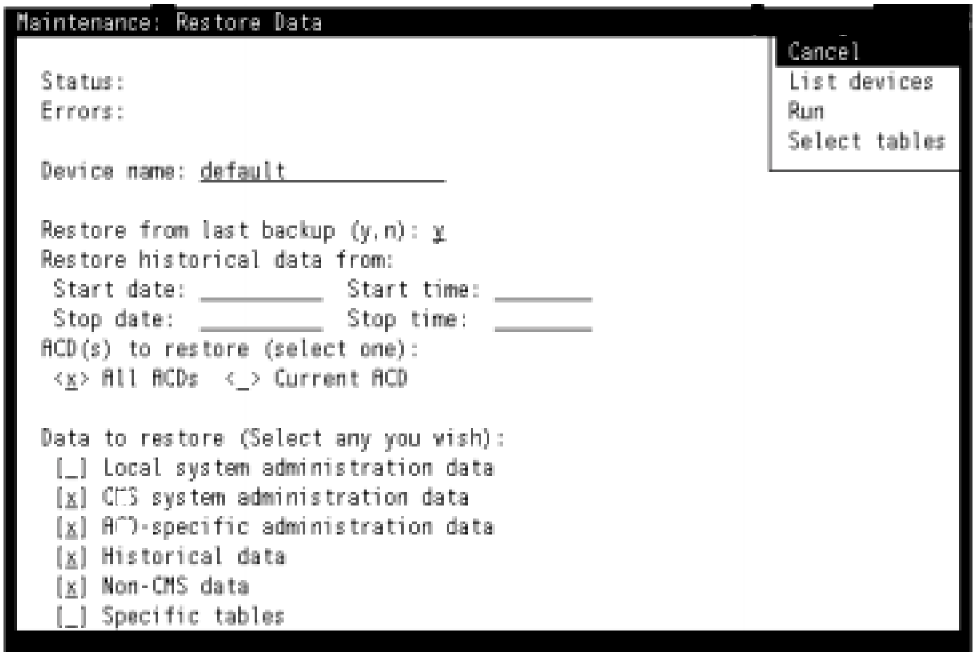
To restore data to the original server:

1. Insert the full maintenance backup tape created on the new HA server into the tape drive on the original server.
2. Log in as a CMS user.

   The **CMS Main Menu** is displayed.
3. From the main menu, select **Maintenance** > **Restore Data**.

   The **Maintenance: Restore Data** window is displayed.

4. In the **Data to Restore** fields, select the **Historical data** and **Non-CMS data** options, as illustrated in the following figure:



```
Maintenance: Restore Data
                                                         Cancel
 Status:                                                 List devices
 Errors:                                                 Run
                                                         Select tables
 Device name: default_____________

 Restore from last backup (y,n): y
 Restore historical data from:
  Start date: __________  Start time: ________
  Stop date:  __________  Stop time:  ________
 ACD(s) to restore (select one):
  <x> All ACDs  <_> Current ACD

 Data to restore (Select any you wish):
  [_] Local system administration data
  [x] CMS system administration data
  [x] ACD-specific administration data
  [x] Historical data
  [x] Non-CMS data
  [_] Specific tables
```

5. After you verify that the correct restore options are selected, press **Enter** to move the active cursor to the action box in the top right corner of the window.

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

   If the customer does not have any custom report tables set up by the PSO, the **Maintenance: Restore Data** window will display the following message when the restore is run:

   ```
   Errors: Initialization errors. See Error Log.
   ```

   To view the error log, select **Maintenance** > **Error Log** from the CMS menu. The relevant log message reads as follows:

   ```
   Restore process startup failed. Cannot restore non-CMS data
   because there are not tables in the database for that group.
   ```

   These error messages can be ignored.

CMSADM backups on the HA servers

When both servers are fully operative, CMSADM backups must be performed as soon as possible on each server. The CMSADM file system backup saves all system files (excluding CMS call data). You must store these backups in a safe place so they can be used to restore the system after a major system failure.

For a description of the CMSADM backup procedure, see Performing a CMSADM backup on page 25.

Administering the switch for CMS HA systems

Before an Avaya^{TM} Call Management System (CMS) high availability (HA) system can collect and process Automatic Call Distribution (ACD) data from the switch, you must administer a hardware interface on the switch. Each switch can use a number of different interfaces to communicate to a CMS computer.

For detailed information about switch administration, see “Administering the switch link” in *Avaya CMS Switch Connections Administration and Troubleshooting*, 585-215-876.

Index