Avaya Call Management System
High Availability
Connectivity, Upgrade and Administration
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.

Trademarks

Avaya is a trademark of Avaya Inc.
DEFINITY is a registered trademark of Avaya.
All non-Avaya trademarks are the property of their respective owners.

Document ordering information:

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: Document No. 07-300065, Issue 1.0
June 2004

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 102563.

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

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 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).
## Contents

**Preface**  
Purpose ................................................. 5  
Intended users ........................................ 6  
Overview ................................................. 6  
Conventions and terminology ...................... 7  
Reasons for reissue .................................. 7  
Availability ............................................ 8  
Related documentation ................................ 9  
Change description .................................... 9  
Software documents ................................... 9  
Administration documents ............................ 10  
Avaya CMS upgrade documents ....................... 10  
  Base load upgrades .................................. 10  
  Platform upgrades and data migration .......... 11  
  Avaya Call Management System Upgrade Express (CUE) 11  
Hardware documents .................................. 12  
Communication Manager documents ................. 12  
Documentation Web sites .............................. 13  
Support .................................................. 14  

**Introduction** ........................................ 15  
About CMS HA ........................................... 16  
Supported communication servers ................. 17  
Supported CMS platform combinations .......... 17  
Recommendations for HA configurations with different Sun platforms 18  
Required and optional software .................. 18  
Special upgrade considerations ................... 19  
General roles and responsibilities ............... 19  
Customer-specific roles and responsibilities .... 20  

**Connecting HA servers to the communication server** ............ 21  
  Basic configuration rules .......................... 21  
  Ethernet ports on a CMS server .................. 22  
  Server switch-over options ....................... 23
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 5
- **Intended users** on page 6
- **Overview** on page 6
- **Conventions and terminology** on page 7
- **Reasons for reissue** on page 7
- **Availability** on page 8
- **Related documentation** on page 9
- **Support** on page 14

---

Purpose

The purpose of this document is to describe how to install and maintain your CMS High Availability (HA) system.
Preface

Intended users

This document is written for:
- Software specialists
- 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 15
  Provides an overview of CMS HA.
- **Connecting HA servers to the communication server** on page 21
  Provides connectivity requirements and recommendations specific to CMS High Availability (HA) systems.
- **Upgrading CMS to the High Availability option** on page 25
  Provides upgrade procedures used to combine a new CMS server with an existing CMS system in order to create a CMS High Availability (HA) system.
Conventions and terminology

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

Unless otherwise specified, all information and procedures in this document apply to the Sun Enterprise 3500, Sun Fire V880, Sun Blade 100, and Sun Blade 150.

Unless specified otherwise, the term CMS always implies Avaya Call Management System.

Unless specified otherwise, the term Sun Blade always implies Sun Blade 100 or Sun Blade 150.

The term communication server refers to an Avaya switch.

Reasons for reissue

This is the first issue of this document.
Availability

Copies of this document are available from one or both of the following sources:

Note:
Although there is no charge to download documents through the Avaya Web site, documents ordered from the Avaya Publications Center must be purchased.

- The Avaya online support Web site, http://www.avayadocs.com
- The Avaya Publications Center, which you can contact by:
  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)

  Mail:
  GlobalWare Solutions
  200 Ward Hill Avenue
  Haverhill, MA 01835 USA
  Attention: Avaya Account Manager

  E-mail:
  totalware@gwsmail.com
Related documentation

You might find the following Avaya CMS documentation useful. This section includes the following topics:

- Change description on page 1
- Software documents on page 1
- Administration documents on page 1
- Avaya CMS upgrade documents on page 1
- Hardware documents on page 1
- Communication Manager documents on page 1
- Documentation Web sites on page 1

Change description

For information about the changes made in Avaya CMS R12, see:

- Avaya Call Center 2.1 and CMS Release 12 Change Description, 07-300197

Software documents

For more information about Avaya CMS software, see:

- Avaya CMS Open Database Connectivity, 585-780-701
- Avaya Call Management System Release 12 External Call History Interface, 07-300064
- Avaya CMS Custom Reports, 585-215-822
- Avaya CMS Forecast, 585-215-825
- Avaya Visual Vectors Release 12 Installation and Getting Started, 07-300069
Administration documents

For more information about Avaya CMS administration, see:

- Avaya Call Management System Release 12 Administration, 07-300062
- Avaya Call Management System Database Items and Calculations, 07-300011
- Avaya CMS Supervisor Release 12 Reports, 07-300012
- Avaya CMS Supervisor Release 12 Installation and Getting Started, 07-300009
- Avaya Call Management System High Availability User Guide, 07-300065
- Avaya Call Management System High Availability Connectivity, Upgrade and Administration, 07-300065

Avaya CMS upgrade documents

There are several upgrade paths supported with Avaya CMS. There is a document designed to support each upgrade. None of the following upgrade documents are available from the publications center.

This section includes the following topics:

- Base load upgrades on page 1
- Platform upgrades and data migration on page 1
- Avaya Call Management System Upgrade Express (CUE) on page 1

Base load upgrades

Use a base load upgrade when upgrading CMS to the latest load of the same version (for example, R3V9 ak.g to R3V9 al.k). A specific set of instructions is written for the upgrade and is shipped to the customer site with the CMS software CD-ROM as part of a Quality Protection Plan Change Notice (QPPCN).

For more information about base load upgrades, see:

- Avaya CMS R12 Base Load Upgrades
Platform upgrades and data migration

Use a platform upgrade when upgrading to a new hardware platform (for example, upgrading from a SPARCserver 5 to a Sun Blade 150). The new hardware platform is shipped from the Avaya factory with the latest CMS load. Therefore, as part of the upgrade you will have the latest CMS load (for example, R3V9 to R12 or the latest load of the same CMS version). For R12, a specific set of instructions is written for the upgrade and is shipped to the customer site with the new hardware.

For more information about platform upgrades and data migration, see:

- Avaya Call Management System Release 12 Platform Upgrade and Data Migration, 07-300067

Avaya Call Management System Upgrade Express (CUE)

Use CUE in the following conditions:

- CMS is being upgraded from an earlier version (for example R3V6) to the latest version (for example, R12).
- The hardware platform is not changing.

A specific set of upgrade instructions is written for the upgrade and is shipped to the customer site with the CUE kit.

For more information about CUE upgrades, see:

- Avaya Call Management System (CMS) Release 12 CMS Upgrade Express (CUE) Customer Requirements, 07-300010
- Avaya Call Management System Release 12 Sun Blade 100 Workstation CMS Upgrade Express
- Avaya Call Management System Release 12 Sun Blade 100 Workstation Mirrored System CMS Upgrade Express
- Avaya Call Management System Release 12 Sun Enterprise 3500 Computer CMS Upgrade Express
- Avaya Call Management System Release 12 Sun Enterprise 3500 Computer Mirrored System CMS Upgrade Express
- Avaya Call Management System Release 12 Sun Fire V880 Computer CMS Upgrade Express
Hardware documents

For more information about Avaya CMS hardware, see:

- **Avaya Call Management System Sun Fire V880 Computer Hardware Installation, Maintenance, and Troubleshooting**, 585-215-116
- **Avaya Call Management System Sun Fire V880 Computer Connectivity Diagram**, 585-215-612
- **Avaya Call Management System Sun Blade 100/150 Computer Hardware Installation, Maintenance, and Troubleshooting**, 585-310-783
- **Call Management System Sun Blade 100/150 Computer Connectivity Diagram**, 585-310-782
- **Avaya Call Management System Sun Enterprise 3500 Computer Hardware Installation, Maintenance, and Troubleshooting**, 585-215-873
- **Call Management System Sun Enterprise 3500 Computer Connectivity Diagram**, 585-215-877
- **Avaya Call Management System Terminals, Printers, and Modems**, 585-215-874

Communication Manager documents

For more information about Avaya CMS communication servers, see:

- **Avaya Call Management System Switch Connections, Administration, and Troubleshooting**, 585-215-876
- **Avaya Communication Manager Call Center Software - Call Vectoring and Expert Agent Selection (EAS) Guide**, 07-300186
- **Avaya Communication Manager Call Center Software - Automatic Call Distribution (ACD) Guide**, 07-300185
- **Avaya Communication Manager Call Center Software - Basic Call Management System (BCMS) Operations**, 07-300061
Documentation Web sites

For product documentation for all Avaya products and related documentation, go to http://www.avayadocs.com. Additional information about new software or hardware updates will be contained in future issues of this book. New issues of this book will be placed on the 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

- Okidata printer documentation
  http://www.okidata.com

- Informix documentation
  http://www.informix.com

- Tivoli Storage Manager documentation
  http://www.tivoli.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.

Information required for High Availability technical support
Identify yourself as a Avaya CMS High Availability customer and be prepared to give the following information:

- Your full name, your organization, and a phone number where an Avaya representative can contact you about the problem
- The installation location (IL) number
  The IL number is a 10-digit number that helps identify the details of your Avaya CMS High Availability installation and environment
- Your ACD and CMS release information
- Whether the problem is with the primary CMS server or the secondary CMS server
- CPU type and speed
- Microsoft Windows operating system version (if using Avaya CMS Supervisor)
- A description of the problem
- The type of service contract your organization has with Avaya, if any
- Whether you have a Business Communication Solutions and Integration (BCSI) contract related to the High Availability option
  If your system is not covered by warranty or a service contract, you will be charged for the Helpline troubleshooting. If you are uncertain about the details or expiration date of your service contract, contact your Avaya sales representative.
Introduction

The Avaya 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.

This section includes the following topics:

- About CMS HA on page 16
- Supported communication servers on page 17
- Supported CMS platform combinations on page 17
- Recommendations for HA configurations with different Sun platforms on page 18
- Required and optional software on page 18
- Special upgrade considerations on page 19
- General roles and responsibilities on page 19
- Customer-specific roles and responsibilities on page 20
About CMS HA

The CMS HA configuration includes features associated with the Automatic Call Distribution (ACD) feature of Avaya communication servers operating in conjunction with the CMS software application. The CMS HA configuration consists of the following major features:

● Dual Automatic Call Distribution (ACD) links on the communication server

● 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 configuration 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 communication server over separate TCP/IP over Ethernet subnets.

The CMS servers installed in HA configurations 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 automatically by the Auto-sync feature from Avaya BCSI that is installed in every HA configuration. For a manual synchronization process, customers can also copy a full maintenance backup from the primary server to the secondary server, or manually make 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 BCSI, 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 previously, 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 communication servers

The CMS HA option is currently supported on the following Avaya communication servers:

- DEFINITY ECS with R8.x, R9.x, R10.x
- DEFINITY servers with Communication Manager Call Center Software
- S8100 Media Server with Communication Manager Call Center Software
- S8300 Media Server with Communication Manager Call Center Software
- S87xx Media Server with Communication Manager Call Center Software

Additional communication servers might be supported depending on your CMS load. For more information contact your Avaya sales or support representative.

Supported CMS platform combinations

Some platforms might require additional hardware or software upgrades in order to be used in a HA configuration.

CMS HA is currently supported on the following platform combinations:

- Sun Enterprise 3500 - Sun Enterprise 3500
- Sun Fire V880 - Sun Fire V880
- Sun Blade 100 - Sun Blade 100
- Sun Blade 150 - Sun Blade 150
- Sun Blade 150 - Sun Blade 100
- Sun Fire V880 - Sun Enterprise 3500

Different platform combinations might be supported depending on your CMS load. For more information contact your Avaya sales or support representative.

Note:

If one of the CMS servers has a DAT 72 tape drive and the other CMS server has a DDS-4 tape drive, you must use DDS-4 tape cartridges on both servers for backups. Do not use the DAT 72 tapes for backups on either one of the servers. If both servers have DAT 72 tape drives, you can use DAT 72 tapes for backups.
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 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 Sun Blade 150 and Sun Blade 100 servers are combined, the Sun Blade 150 server should be designated as the primary server.

Note:
If one of the CMS servers has a DAT 72 tape drive and the other CMS server has a DDS-4 tape drive, you must use DDS-4 tape cartridges on both servers for backups. Do not use the DAT 72 tapes for backups on either one of the servers. If both servers have DAT 72 tape drives, you can use DAT 72 tapes for backups.

Required and optional software

A complete set of CMS 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 configurations, the following exceptions to the standard CMS software configurations apply:

- X.25 software is not supported as the final connection link between the communication server and the HA servers or with CMS loads Release 12 or later. X.25 can be used to connect remote communication servers to an on site communication server.
- 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 configuration 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 synchronization between the primary and secondary servers is a key maintenance requirement for HA configurations, 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, BCSI must be contacted before the upgrade process is initiated.

For further details of the CMS upgrade process, see Upgrading CMS to the High Availability option on page 25.

General roles and responsibilities

The following table lists the major tasks for each communication server type, the location of the procedure in the book, and who is responsible for performing each task.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Task</th>
<th>Technician</th>
<th>TSC</th>
<th>Software specialist</th>
<th>Customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Connecting the communication server</td>
<td>X</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>Administering CMS</td>
<td>N/A</td>
<td>N/A</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>Administering the communication server</td>
<td>N/A</td>
<td>N/A</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>N/A</td>
<td>Troubleshooting communication server</td>
<td>X</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

For information about troubleshooting communication server connections, see the Avaya CMS switch connections, administration, and troubleshooting document.
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.

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retention of CMS documentation and software</td>
</tr>
<tr>
<td>For those administration changes that are non-transferable via backup tape, revision on each HA server</td>
</tr>
<tr>
<td>Nightly full maintenance backups on the primary server</td>
</tr>
<tr>
<td>Nightly full maintenance restores on the secondary server</td>
</tr>
<tr>
<td>Monthly (or more frequent) CMSADM backups on the primary server</td>
</tr>
<tr>
<td>Checking log records to verify success of backup</td>
</tr>
</tbody>
</table>
Connecting HA servers to the communication server

This section describes connectivity requirements and recommendations specific to CMS High Availability (HA) systems. For more information on supported communication servers, see, Supported communication servers on page 17.

The connectivity configurations described in this chapter represent the optimal link setups for HA configurations. For detailed connectivity diagrams, see the section on connecting a switch link in the Avaya CMS switch connections, administration, and troubleshooting document.

This section includes the following topics:

- Basic configuration rules on page 21
- Server switch-over options on page 23

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 communication servers. 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 communication server.

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 communication server. The communication server 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 configurations, see the section on administering a switch link in the Avaya CMS switch connections, administration, and troubleshooting document.
Connecting HA servers to the communication server

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 should be dedicated solely to the communication server link.

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

Local communication server 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 the Avaya CMS switch connections, administration, and troubleshooting document.
Server switch-over options

The primary purpose of the CMS High Availability offer is to ensure an uninterrupted data stream between the communication server 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:

**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.

**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 BCSI representatives in order to discuss logistical issues associated with manual server switch-overs.
Connecting HA servers to the communication server
Upgrading CMS to the High Availability option

This section describes Avaya 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) configuration.

This section includes the following topics:

- Terminology on page 25
- Upgrade scenarios on page 26
- CMS software combinations on page 27
- Procedures for an HA upgrade on page 28
- Setting up CMS on an HA server on page 40
- Finalizing the upgrade on page 45

Terminology

The two CMS servers used to build an HA configuration 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
Upgrade scenarios

The CMS servers used in an HA configuration must have the same CMS version and base load number. If the original server has a different CMS version from the new HA server being added to the system, upgrade of the original server must be performed using one of the following upgrade processes:

**Base load upgrade** - this should be used when the original server is on the same CMS release (for example, R12), but is one base load older than the new HA server. See the *Avaya CMS Base Load Upgrades* document for the appropriate base load.

**CMS Upgrade Express (CUE)** - This should be used when the original server is on an older release of CMS (for example, R3V9) and the new HA server is the latest release of CMS (for example, R12). See the *Avaya CMS Upgrade Express* document for your particular upgrade.

**Platform upgrade** - This should be used when the original server is on a platform that is no longer supported with the latest CMS release (for example, CMS R12 does not support the Enterprise 3000). In this example, the old server must be replaced with a new platform that supports CMS R12. See the *Avaya CMS Platform Upgrade and Data Migration* document for your particular upgrade.
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

This section includes the following topics:

- Things to consider if the servers have the same CMS version on page 27
- Things to consider if the servers have different CMS versions on page 27

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 configuration are greatly simplified because:

- The communication server 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 communication server 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 configuration 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.
Procedures for an HA upgrade

This section presents an overview of the steps required to upgrade the CMS version of the original 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 Base Load Upgrades.

This section includes the following topics:

- Prerequisites on page 28
- Steps to perform 24 hours before the upgrade on page 29
- Steps to perform the day of the upgrade on page 30
- Verifying the tape drive on the server currently in service on page 33
- Performing a CMSADM backup on page 34
- Performing a full maintenance backup on page 36
- Performing a maintenance backup of only the administration data on page 37

Prerequisites

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

Contact Avaya BCSI to schedule installation of the Auto-sync feature on both the original server and the new HA server.
Steps to perform 24 hours before the upgrade

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

1. Upgrade the communication servers to the new compatible release and administer the communication servers 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 R3V11, then upgrade the communication server and administer it to communicate with an R3V11 CMS.

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 33.

   Note:
   
   If the tape drives between the original HA server and the new HA server are not the same, you must use the Remote Tape Copy (RTC) feature to transfer backup data as described in Avaya CMS Platform Upgrade and Data Migration.

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 17.

   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 34 and Performing a full maintenance backup on page 36.
Steps to perform the day of the upgrade

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

1. The Avaya technician arrives on site and performs a backup of system and ACD-specific administration data on the original server (see Performing a maintenance backup of only the administration data on page 37).

⚠️ 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 29 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 communication servers and re-administer the ACD links for the CMS load and dual ACD links.

4. If the CMS configuration includes data collection by Avaya Operational Analyst (OA), turn off all Avaya OA forwarders on the original server using the `dcrun off cms fwd` command.

5. As soon as the communication server is re-administered, release the busy out for the links. When 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.

6. If the CMS configuration includes data collection for Avaya OA, turn on all Avaya OA forwarders using the `dcrun on cms fwd` command.

7. Perform an incremental maintenance backup on the original server (historical data only), and then turn off the system.

8. Upgrade the original server using one of the following processes as described in Upgrade scenarios on page 26:

   - Base load upgrade
   - CUE upgrade
   - Platform upgrade

9. After the 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.

10. If the CMS configuration includes data collection for Avaya OA, turn on all Avaya OA forwarders using the `dcrun on cms fwd` command.

11. Migrate the CMS historical data from the incremental maintenance backup (Step 7) 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 29 and migrate all of the remaining historical data to the new HA server.

12. 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.

13. Run a full maintenance backup on the new HA server. For more information, see Performing a full maintenance backup on page 36.

14. Restore the historical data from the full maintenance backup tape (created in Step 13) 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.

15. Run CMSADM backups on both servers.

16. Continue with Setting up CMS on an HA server on page 40.

For more information, see the Schematic of HA upgrade process on page 32 and Avaya / CMS High Availability User Guide.
Schematic of HA upgrade process

The following graphic is a 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

Legend

- Data collection on
- Data collection off
Verifying the tape drive on the server currently in service

New systems are currently offered with the DAT 72 or DDS-4 4mm tape drive. If one of the CMS servers has a DAT 72 tape drive and the other CMS server has a DDS-4 tape drive, you must use DDS-4 tape cartridges on both servers for backups. Do not use the DAT 72 tapes for backups on either one of the servers. If both servers have DAT 72 tape drives, you can use DAT 72 tapes for backups.

Use the following procedures to determine the model of tape drive installed on each server.

To determine if you have a DAT 72 tape drive:

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

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

   If the tape drive is a DAT 72, a message similar to the following is displayed:

   ```
   HP DAT-72 tape drive:
   sense key(0x6)= Unit Attention residual= 0 retries= 0
   file no= 0 block no= 0
   ```

To determine if you have a DDS-4 tape drive:

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

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

   If the tape drive is a DDS-4, a message similar to the following is displayed:

   ```
   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

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 configuration, the customer must perform a CMS full maintenance backup within 24 hours of starting the HA upgrade process.

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.

   1. To accept the default backup options, press **Enter** to activate the action list in the upper right corner of the window.

   2. 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.

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**.
Upgrading CMS to the High Availability option

⚠ 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:

```
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

RCD(s) to back up (Select one):
<x> All RCDs  <_> Current RCD

Data to back up (Select any you wish):
[ ] Local system administration data
[x] CMS system administration data
[ ] ACD-specific administration data
[ ] Historical data,
   Select one:
   <_> Full  <_> Incremental
[ ] 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, perform the following steps:
   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: \texttt{q}

   The system responds:

   \begin{verbatim}
   Enter device path:
   \end{verbatim}

   c. Enter the device path for the tape drive.

   Example:

   \begin{verbatim}
   /dev/rmt/0c
   \end{verbatim}

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

   \begin{verbatim}
   Enter 1 to list the tables or v to also verify the volume:
   \end{verbatim}

   d. Enter: \texttt{1}

   The system displays a list of the database tables included on the backup.
Setting up CMS on an HA server

This section refers to procedures that apply to both the original server and new HA 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.

This section includes the following topics:

- [Prerequisites](#) on page 41
- [Setting CMS authorizations](#) on page 41
- [Setting up data storage parameters](#) on page 42
- [Setting up a LAN for communication server connections](#) on page 42
- [Setting Up the CMS application](#) on page 43
- [Installing feature packages](#) on page 43
- [Setting up the remote console](#) on page 44
- [Setting up the Alarm Origination Manager](#) on page 44
- [Setting up the NTS](#) on page 44
- [Creating an alternate boot device for mirrored systems](#) on page 44
Prerequisites

The TSC should verify that:

● A copy of the appropriate Avaya CMS software installation, maintenance and troubleshooting document for your CMS release is available for reference
● A copy of the CMS switch connections administration and troubleshooting document is available for reference
● A copy of the CMS terminals printers and modems document 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 communication server.

⚠️ 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 communication server. For communication server administration procedures, see the section on administering the switch link in the CMS switch connections administration and troubleshooting document.

● The NTS and the CMS computer are connected to the network hub unit. For more information, see the CMS terminals printers and modems document.

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 the section on setting up CMS authorizations in the appropriate CMS software installation, maintenance and troubleshooting document for your CMS release.
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 configuration 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 the appropriate CMS software installation, maintenance and troubleshooting document for your CMS release.

Setting up a LAN for communication server connections

This section contains information about setting up a LAN connection between the CMS computer and one or more HA-enabled communication servers. This type of connection is used only with communication server Release 8.1 or later. The LAN connections described herein are based on the configuration recommended for HA configurations, 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 communication server, you must coordinate the administration done on the CMS computer with the administration done on the communication server 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 the appropriate CMS software installation, maintenance and troubleshooting document for your CMS release.
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 the appropriate CMS software installation, maintenance and troubleshooting document for your CMS release.

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 the appropriate CMS software installation, maintenance and troubleshooting guide for your CMS release.

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 Avaya BCSI, 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 BCSI, 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 the sections on setting up the remote console and redirecting the remote console port to the modem in the appropriate 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 the section on setting up the alarm origination manager in the appropriate CMS software installation, maintenance and troubleshooting guide.

Setting up the NTS

For information about setting up the NTS, see the section on setting up the NTS in the CMS terminals, printers, and modems document.

Creating an alternate boot device for mirrored systems

This procedure creates an alternate boot device. This procedure is required only for platforms configured as mirrored systems. For a description of the procedure used to create the alternate boot device, see the section on creating an alternate boot device for mirrored systems in the appropriate CMS software installation, maintenance and troubleshooting document.
Finalizing the upgrade

The following procedures describe how to finalize the upgrade:

- **Migrating CMS system administration data to the new HA server** on page 45
- **Checking the archive interval** on page 47
- **Administering the communication server** on page 48
- **Performing an incremental maintenance backup** on page 49
- **Migrating CMS historical data to the new HA server** on page 50
- **Migrating administration data back to the original server** on page 51
- **Performing a new full maintenance backup and restore** on page 53
- **CMSADM backups on the HA servers** on page 55

---

**Migrating CMS system administration data to the new HA server**

This section uses the maintenance backup tape which was created during the procedure described in **Performing a maintenance backup of only the administration data** on page 37. 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 36 for this migration.

For all supported versions of CMS, 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

Device name: default

Data type (Select one):
  <> System Administration data (single-user required)
  <> Agent/Call Center Admin data (single-user required)
  <> Historical data

Stop date: 
Stop time: 11:39 PM

Specify FCD(s) to migrate (Select one):
  <> All ACDs
  <> Single FCD
      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.

```
      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
```

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 communication server**

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

For details of communication server administration for HA configurations, see the section on administering the switch link in the CMS switch connections administration and troubleshooting document.

After you have re-administered the communication server, 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 communication server 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.

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:

   ![Backup Selections Example](image)

   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.
Migrating CMS historical data to the new HA server

After the communication server 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 49) to the new HA server.

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 window](image)

   - Data type (Select one):
     - System Administration data (single-user required)
     - Agent/Call Center Admin data (single-user required)
     - Historical data
     - Stop date: __________
     - Stop time: __:__ PM

   - Specify ACD(s) to migrate (Select one):
     - All ACDs
     - Single ACD
     - from: ___ to: ___

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](#)) 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](#)) 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.

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:

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`. 

---

52  Avaya CMS High Availability Connectivity, Upgrade and Administration
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.

This section includes the following topics:

- Performing the full maintenance backup on the new HA server on page 53
- Restoring historical data to the original server on page 53

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 36.

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 configuration. 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.

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](image)

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 BCSI, 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 34.
Upgrading CMS to the High Availability option
Index

A
administering
  communication server LAN ........................................... 42
  TCP/IP ........................................................................ 42
Alarm Origination Manager ............................................... 44
archive interval, checking .................................................. 47

B
backup
  admin data ..................................................................... 37
  CMSADM ....................................................................... 34
  full maintenance ............................................................ 36
  incremental maintenance .................................................. 49

C
CMS
  application setup .......................................................... 43
  authorizations, setting ....................................................... 41
  data storage parameters .................................................... 42
  feature packages ............................................................ 43
  setting up on HA servers .................................................. 40
communication server
  administration .................................................................. 48
  link ................................................................................ 42
  TCP/IP .......................................................................... 42
  configuration rules ............................................................ 21

E
Ethernet ports ................................................................. 22

F
FSBE ............................................................................. 22

H
helplines ......................................................................... 14
High Availability, defined ................................................. 23

L
LAN
  overview ........................................................................ 42

M
migration
  administration data .......................................................... 51
  CMS historical data .......................................................... 50
  CMS system admin data .................................................... 45
mirrored systems
  alternate boot device .......................................................... 44

N
NTS
  administration ................................................................. 44
  setup ............................................................................. 44

P
platforms
  combinations supported by High Availability ...................... 17
  supported HA combinations .............................................. 17
ports, Ethernet
  on CMS computers .......................................................... 22
primary server
  defined ........................................................................ 16
  installed software ............................................................. 16

R
remote console
  set up ........................................................................... 44
  setting up the software ...................................................... 44
restore, historical data ........................................................... 53
roles and responsibilities
  customer ...................................................................... 20
  technical support personnel .............................................. 19

S
secondary server
  defined ........................................................................... 16