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

Documentation disclaimer
Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

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

Warranty
Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:
http://www.avaya.com/support

Preventing toll fraud
"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, anyone who is not a corporate employee, agent, subcontractor, or person 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 assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya 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).

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

Document ordering information:
Avaya Publications Center

Voice:  +1-207-866-6701
Fax:  +1-207-626-7269

Order:  Document No. 07-300066, Issue 2.0

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 102568.

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
Avaya Call Management System
High Availability User Guide

Contents

Preface .................................................................................................................. 7
  Purpose ........................................................................................................... 7
  Intended users ............................................................................................... 8
  Overview ....................................................................................................... 8
  Conventions and terminology .................................................................... 9
  Reasons for reissue ..................................................................................... 9
  Availability .................................................................................................. 10
  Related documentation ............................................................................. 11
    Change description .................................................................................. 11
    Software documents ............................................................................... 11
    Administration documents .................................................................... 12
    Hardware documents ............................................................................ 12
    Call Center documents ......................................................................... 12
    Avaya CMS upgrade documents ............................................................ 13
      Base load upgrades ............................................................................... 13
      Platform upgrades and data migration .............................................. 13
      Avaya Call Management System Upgrade Express (CUE) .............. 13
    Documentation Web sites ..................................................................... 14
  Support ......................................................................................................... 15

Introduction ........................................................................................................ 17
  HA server switch-over after a failure event .............................................. 18
  Dual ACD links .......................................................................................... 19
  CMS feature enhancements ...................................................................... 20
  Increased data availability ......................................................................... 21

Primary and secondary CMS servers .............................................................. 23
  CMS HA server maintenance .................................................................... 25
  CMS recovery kit ...................................................................................... 26
  Recovery kit contents ............................................................................... 26
  Recovery kit software components .......................................................... 26
  Connectivity considerations for CMS server switch-overs ...................... 28
  Administration operations auto-synchronized by the communication server .................................................................................. 28
  Administration operations requiring manual synchronization .......... 29
  Administration operations synchronized by backups and restores ......... 31
  Operations requiring data collection to be turned off ............................ 32
User scenarios .......................................................... 33
  Modifying agent trace ........................................... 34
  Upgrading the CMS base load .................................. 34
  Modifying call work codes ..................................... 35
  Modifying agent skills ......................................... 35
  Creating custom reports ....................................... 35
  Creating designer reports ...................................... 36
  Modifying the Dictionary ....................................... 37
  Administering exceptions ..................................... 40
  Turning External Call History on and off .................. 40
  Administering forecast data storage allocation .......... 41
  Administering Forecasting report data ..................... 41
  Synchronizing main menu additions ......................... 42
  Administering printers ........................................ 42
  Scripting .......................................................... 43
    Interactive scripts ........................................... 43
    Automatic scripts ............................................ 43
  Administering shortcuts ...................................... 43
  Setting up the split/skill call profile ....................... 44
  Synchronizing after data collection is turned on/off .... 45
    Worksheet for synchronizing the CMS servers after turning data collection on/off .................. 46
    Diagram of synchronizing CMS servers after data collection is turned on/off ............... 48
  Running timetables only on the primary server .......... 49
  Running timetables on both primary and secondary servers ............................................. 51
  Globally editing timetables to change server ownership ............................................. 52
  Adding or modifying users .................................... 54
  Removing users .................................................. 54
  Setting user passwords ........................................ 55
  Administering the VDN call profile ......................... 56
  Administering Avaya Visual Vectors ......................... 57

High Availability backup and restore strategy .................. 59
  Synchronizing after an unscheduled outage of the primary CMS server ......................... 60
  Synchronizing after an unscheduled outage of the secondary CMS server ....................... 61

Appendix A: CMS backups and restores .......................... 63
  Backup and restore procedures .............................. 63
  Avaya CMS backup strategy .................................... 64
    Labeling the backup volume ................................ 64
    Backup information format ................................ 64
    How to interpret backup information ..................... 65
<table>
<thead>
<tr>
<th>Appendix B: Items excluded from a CMSADM backup</th>
<th>67</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix C: Items backed up during a full maintenance backup</td>
<td>69</td>
</tr>
<tr>
<td>Appendix D: Restore characteristics of different data types</td>
<td>73</td>
</tr>
<tr>
<td>Appendix E: What to do if an Avaya CMS server fails.</td>
<td>75</td>
</tr>
<tr>
<td>Primary CMS server</td>
<td>75</td>
</tr>
<tr>
<td>Secondary CMS server</td>
<td>76</td>
</tr>
<tr>
<td>Both CMS servers</td>
<td>76</td>
</tr>
<tr>
<td>Appendix F: Frequently asked questions</td>
<td>77</td>
</tr>
<tr>
<td>Appendix G: Avaya CMS base load upgrade procedure for High Availability systems</td>
<td>79</td>
</tr>
<tr>
<td>Index</td>
<td>81</td>
</tr>
</tbody>
</table>
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 7
- **Intended users** on page 8
- **Overview** on page 8
- **Conventions and terminology** on page 9
- **Reasons for reissue** on page 9
- **Availability** on page 10
- **Related documentation** on page 11
- **Support** on page 15

Purpose

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

This document is written for:

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

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

Overview

This document includes the following topics:

- **Introduction** on page 17
  
  Provides an overview of an Avaya HA system.

- **Primary and secondary CMS servers** on page 23
  
  Outlines the Avaya HA maintenance procedures.

- **User scenarios** on page 33
  
  Describes how to perform normal CMS tasks in a HA configuration.

- **High Availability backup and restore strategy** on page 59
  
  Describes how to recover a HA system after an unscheduled outage.
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 Fire V890, 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.

Unless specified otherwise, the term Sun Fire always implies Sun Fire V880 or Sun Fire V890.

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](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 11
● Software documents on page 11
● Administration documents on page 12
● Hardware documents on page 12
● Call Center documents on page 12
● Avaya CMS upgrade documents on page 13
● Documentation Web sites on page 14

Change description

For information about the changes made in Avaya CMS R13, see:

● Avaya Call Center 3.0 and Call Management System (CMS) Release 13 Change Description, 07-300304

Software documents

For more information about Avaya CMS software, see:

● Avaya Call Management System Release 13 Software Installation, Maintenance, and Troubleshooting Guide, 07-300340
● Avaya CMS Open Database Connectivity Version 4.2, 585-780-701
● Avaya Call Management System Release 13 External Call History Interface, 07-300332
● Avaya CMS Custom Reports, 585-215-822
● Avaya Visual Vectors Release 13 Installation and Getting Started, 07-300353
● Avaya Call Management System (CMS) Supervisor Release 13 Report Designer, 07-300335
Administration documents

For more information about Avaya CMS administration, see:

- Avaya Call Management System Release 13 Administration, 07-300331
- Avaya Call Management System (CMS) Release 13 Database Items and Calculations, 07-300330
- Avaya Call Management System Supervisor Release 13 Reports, 07-300334
- Avaya Call Management System (CMS) Supervisor Release 13 Installation and Getting Started, 07-300333
- Avaya Call Management System High Availability User Guide, 07-300066
- Avaya Call Management System High Availability Connectivity, Upgrade and Administration, 07-300065

Hardware documents

For more information about Avaya CMS hardware, see:

- Avaya Call Management System Sun Fire V880/V890 Computer Hardware Installation, Maintenance, and Troubleshooting, 585-215-116
- Avaya Call Management System Sun Blade 100/150 Workstation Hardware Installation, Maintenance, and Troubleshooting, 585-310-783
- Avaya Call Management System Terminals, Printers, and Modems, 585-215-874

Call Center documents

For more information about Avaya Call Center documents, see:

- Avaya Communication Manager Call Center Software Basic Call Management System (BCMS) Operations, 07-300061
- 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, 07-300303
- Avaya Communication Manager Call Center Software Automatic Call Distribution (ACD) Guide, 07-300301
Avaya CMS upgrade documents

There are several upgrade paths supported with Avaya CMS. There is a document designed to support each upgrade.

This section includes the following topics:

- **Base load upgrades** on page 13
- **Platform upgrades and data migration** on page 13
- **Avaya Call Management System Upgrade Express (CUE)** on page 13

**Base load upgrades**

Use a base load upgrade when upgrading CMS to the latest load of the same version (for example, r13ak.g to r13al.k). A specific set of instructions is written for the upgrade. The instructions are shipped to the customer site with the CMS software CD-ROM as part of a Product Correction Notice (PCN).

For more information about base load upgrades, see:

- **Avaya Call Management System Release 13 Base Load Upgrade**

**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 R13).

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

- **Avaya Call Management System Release 13 Platform Upgrade and Data Migration**, 07-300339

**Avaya Call Management System Upgrade Express (CUE)**

Use CUE when CMS is being upgraded from an earlier version (for example, R3V9) to the latest version (for example, R13).

A specific set of upgrade instructions is written for the upgrade. These instructions are included on the CUE software CD-ROM that is shipped to the customer site with the CUE kit.

For information about customer requirements for CUE upgrades, see:

- **Avaya Call Management System Release 13 CMS Upgrade Express (CUE) Customer Requirements**, 700356744
For information about CUE upgrade procedures, see:

- **Avaya Call Management System Release 13 Sun Blade 100/150 Workstation Mirrored and Nonmirrored Systems CMS Upgrade Express (CUE), 07-300481**
- **Avaya Call Management System Release 13 Sun Fire V880/V890 Computer CMS Upgrade Express (CUE), 07-300344**

---

**Documentation Web sites**

For Avaya product documentation, go to [http://www.avayadocs.com](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](http://www.avaya.com)

- Sun hardware documentation
  
  [http://docs.sun.com](http://docs.sun.com)

- Informix documentation
  
  [http://www.informix.com](http://www.informix.com)

- Tivoli Storage Manager documentation
  
  [http://www.tivoli.com](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 primary purpose of the Avaya CMS High Availability (HA) option is to ensure an uninterrupted data stream between the communication server and the CMS system. With HA, two CMS servers are connected to one communication server, thereby eliminating the traditional single point of failure between the CMS and the communication server. Refer to the product documentation for your CMS load for more information about supported communication server releases.

Both CMS servers collect data independently from the communication server. With few exceptions (which will be discussed in detail later), both CMS servers provide full CMS capabilities. If either server fails, loses connection to the communication server, or must be brought down for maintenance, the alternate server can carry the entire CMS activity load. Both CMS servers must be administered with an identical CMS setup (number of ACDs in the configuration, data storage allocation, users, features, and so forth).

The Avaya Business Communication Solutions and Integration (BCSI) organization offers a package that automates the synchronization between the two CMS servers. The auto-sync offer reduces the amount of time needed to maintain the HA servers and is required for most installations. For more information, contact BCSI at:

- In the United States 1-877-927-6662
- Outside the United States +1-303-846-0572

As an alternative to the auto-sync offer, the HA option relies heavily on manual data synchronization between the two CMS servers, as well as on manual administration synchronization. This document provides detailed descriptions of procedures needed to maintain synchronization between the two CMS servers.

This section includes the following topics:

- HA server switch-over after a failure event on page 18
- Dual ACD links on page 19
- CMS feature enhancements on page 20
- Increased data availability on page 21
HA server switch-over after a failure event

For customers who require continuous access to their CMS data, HA systems allow for the redirection of LAN traffic related to CMS clients and peripheral devices from the primary server to the secondary server. Switch-over from the primary server to the secondary server can be performed when the primary server experiences a major failure event. However, an HA switch-over should be performed only when the anticipated down time for the primary server is expected to be significant.

Each call center network is configured according to its own unique specifications. Therefore, each HA customer must develop their own customized criteria and plans for server switch-over events.

The CMS HA option allows the following server switch-over options:

- No switch-over
  
  If you do not require continuous access to your CMS data, you can elect 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 will continue on the secondary server, but you may not be able to access that data until the primary server is restored.

- Manual server switch-over
  
  If you require uninterrupted access to CMS data, server switch-over can be performed manually.

  At a minimum, manual switch-over entails the individual editing of CMS supervisor clients by their individual users in order to redirect them from the primary to the secondary server. Also, if the primary server is connected to one or more NTS servers, significant effort may be required to manually switch the NTS devices over to the secondary server. For more information about manual server switch-overs, see Appendix E: What to do if an Avaya CMS server fails on page 75.
Dual ACD links

Duplicate hardware is a key component of the High Availability system. The function of the duplicate hardware is to eliminate a single point of failure in order to prevent data loss due to hardware failures. The dual ACD link feature addresses ACD link failures and builds on the increased ACD link reliability provided by TCP/IP. A C-LAN circuit pack or an ethernet port provides TCP/IP connectivity between the communication server and the CMS server. Each ACD link requires a separate C-LAN circuit pack or ethernet port which supports different network routes to eliminate as many single points of failure as possible.

The ACD Call Processing software sends duplicate data to both CMS servers simultaneously. Thus, both CMS servers will collect identical real-time, historical, and call record data. Furthermore, both CMS servers are able to perform call center and agent administration, and the results are communicated from the communication server back to both CMS servers. However, we strongly recommend performing administrative functions at only the primary CMS server.

An idealized schematic of the network links between each of the dual ACD CLAN cards on a communication server and their respective CMS HA servers is shown in the following figure.
CMS feature enhancements

The following improvements have been made to the standard CMS offer (R3V8 and later) and apply to all standard CMS platforms. These new features were designed to prevent data loss and improve system availability.

- **Non-disruptive CMSADM backup**

  Non-disruptive CMSADM backup has the ability to perform a CMSADM backup with data collection turned on during the entire CMSADM backup process.

  **Note:**

  Non-disruptive CMSADM restores are not technically feasible and will occur with data collection turned off and CMS turned off. A CMSADM backup copies nearly all system directories and files. For a list of those items excluded from a CMSADM backup, see [Appendix B: Items excluded from a CMSADM backup](#) on page 67.

- **Manually synchronize the two CMS systems**

  The following capabilities were incorporated into CMS to allow you to manually synchronize two independent CMS servers in a High Availability configuration:

  - *non-disruptive maintenance restores* - the ability to perform any of the maintenance restores (except for local system administration) with data collection turned on during the entire maintenance restore process.

  - *non-disruptive R3 migration* - the ability to perform any of the R3 migrations with data collection turned on during the entire migration process. R3 migration is critical to synchronizing data during the upgrade process, such as when database schema changes are required.
Increased data availability

The CMS High Availability option increases the availability of your CMS data by means of the following functions and features:

● **ACD link failures**
  
  In the recommended HA configuration, ACD data is transmitted across different C-LAN circuit packs or ethernet ports within the communication server and across different network subnets, thereby reducing the number of potential single points of failure. If one ACD link fails, data collection continues on the second CMS server. You will use the maintenance backup and restore process to recover the missing data onto the CMS server that was connected to the down ACD link.

● **CMS hardware failures**
  
  The CMS server is duplicated. If a hardware failure occurs on one CMS server, data collection continues on the second CMS server. You will use the maintenance backup and restore process to recover the missing data onto the server that failed. If the CMS system fails, you may need to restore the CMSADM backup. Since the CMSADM backup can be performed with data collection on, it is more likely that you will have a good CMSADM backup and the system can be recovered more quickly.

● **Power failures**
  
  The primary and secondary servers should be separately connected to individual uninterruptible power supplies (UPS) on separate protected power circuits. This configuration ensures that both servers will not be simultaneously disabled due to a localized power failure. However, in the event of an extended power outage, impacted servers should be shut down in order to prevent UPS failure and consequent possible data corruption on the server.

● **CMS software failures**
  
  The CMS software application is duplicated. If the CMS application fails or a CMS data collection process fails on one CMS server, data collection continues on the second server. The maintenance backup and restore process is used to recover the missing data onto the CMS server that experienced the software failure event.

● **CMS maintenance**
  
  Data is not lost during either a CMSADM backup or a maintenance backup. Also, data is also not lost when restoring a maintenance backup, as long as local system administration data is not being restored.
CMS full version upgrades

In a High Availability configuration, one CMS server continues to collect data while the other CMS server is upgraded to the new CMS version. After the first CMS server is upgraded, data collection is turned on for the upgraded CMS server. The second CMS server is then upgraded while the upgraded CMS server continues with data collection turned on. After the second CMS server is upgraded, data collection is turned on for the second CMS server and the data is restored between the two CMS servers. If you upgrade the communication server with a new release, the interval of data loss is limited to the amount of time it takes to administer the latest contact center release on the communication server, and pump-up the ACD link.

For more information, see Upgrading the CMS base load on page 34.
### Primary and secondary CMS servers

When the Avaya CMS High Availability offer is installed, one CMS server is designated as the primary server, and the other is designated as the secondary server. It is highly recommended that you perform administration only on the primary CMS server, and administer the secondary CMS server only when the primary is not functioning. In order to avoid possible confusion, the two servers should be clearly labeled as primary or secondary.

The primary and secondary servers are identical, with the following exceptions:

<table>
<thead>
<tr>
<th>Primary CMS server</th>
<th>Secondary CMS server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Might have Internet Call Center installed</td>
<td>Does not ever have Internet Call Center installed</td>
</tr>
<tr>
<td>Timetables turned on</td>
<td>Timetables turned off, except for incremental and full backup timetables and any others you want to run on both CMS servers. For more information about running timetables, see <a href="#">Running timetables only on the primary server</a> on page 49.</td>
</tr>
</tbody>
</table>

Both CMS servers collect data from the communication server, but operate independently from each other. Both servers provide full CMS capabilities except for the differences listed above. Should either server fail, lose connection to the communication server, or need to be shut down for maintenance, the alternate server can carry the entire CMS activity load.

The following operational practices are strongly recommended:

- Always perform administration functions on the primary CMS server. Performing administration on both servers could lead to synchronization problems and loss of historical and/or administration data.

- No users should be logged into the secondary CMS server while the primary CMS server is operational. If the primary CMS server experiences a failure event, your ability to switch CMS users over to the secondary server will depend on your site-specific switch-over strategy, as discussed in [HA server switch-over after a failure event](#) on page 18.
The benefit to creating and following a routine where you always perform administration on the primary CMS server and transfer (synchronize) the data to the secondary CMS server is that you will be more likely to synchronize your data correctly.

This section includes the following topics:

- CMS HA server maintenance on page 25
- CMS recovery kit on page 26
- Connectivity considerations for CMS server switch-overs on page 28
- Administration operations auto-synchronized by the communication server on page 28
- Administration operations requiring manual synchronization on page 29
- Administration operations synchronized by backups and restores on page 31
- Operations requiring data collection to be turned off on page 32
CMS HA server maintenance

In order to assure that both CMS servers are able to accept and process data correctly from the communication server, the administrator must perform the following functions on a daily basis for both CMS servers:

1. Verify that all links to both CMS servers are up.
2. Verify that archiving is occurring on both CMS servers.
   a. Select Maintenance > Archiving Status from the CMS menu.
   b. Press Enter to access the action list in the top right corner of the Maintenance: Archiving Status window.
   c. Press Enter again to view archive status information for all ACDs.
3. Verify that daily backups have run by selecting Maintenance > Backup Data from the CMS menu.

   At the top of the Maintenance: Backup Data window, information similar to the following example is displayed:

   Backups completed today: 1
   Status: Last backup finished at 10/02/00 00:23:41

4. Check the customer error log on both CMS servers for unusual errors.

The maintenance procedures listed above are not unique to the CMS High Availability offer. Therefore, you are probably already accustomed to performing these maintenance procedures on your previous CMS installation.

⚠️ CAUTION:

Failure to adhere to the maintenance practices listed above may result in:

- Unnecessary loss of CMS data
- Additional administrative charges from Avaya technical support
CMS recovery kit

The recovery kit consists of the backup media and original software that the Avaya service organization needs to restore service to your system when problems occur. Store this kit in a secure location to minimize the time your system is out of service.

This section includes the following topics:

- Recovery kit contents on page 26
- Recovery kit software components on page 26

Recovery kit contents

Your CMS recovery kit should include the following:

- The latest CMSADM file system backup tapes
- The latest full maintenance backup tapes
- The patch CD-ROMs and tapes

Recovery kit software components

A number of software packages are shipped with CMS. It is recommended that you store this software with the recovery kit. Refer to the product software installation guide for your specific CMS release for more information about the specific software and software versions required for system recovery.

CMS requires the following software packages (optional packages are noted):

- Solaris; CD-ROM disks 1 and 2
- Software Supplement for the Solaris Operating Environment CD-ROM, contains:
  - Sun Online Validation Test Suite (VTS)
  - Sun Remote System Control (RSC) software (optional)
  - Sun Fire V880 backplane firmware upgrade package (required for Sun Fire V880 platforms)
- CMS Hardware Drivers CD-ROM (optional)
- Annex Communication Server R10.0(B) Annex Host Tools CD-ROM (required only for systems using Network Terminal Server [NTS]). NTSS are not supported with Solaris 9.
- Informix SQL CD-ROM (optional)
- Informix IDS CD-ROM
- Informix ESQL SDK CD-ROM
- Informix ILS CD-ROM
- Avaya CMS Supplemental Services R12 CD-ROM
- Avaya Call Management System Release 12 CD-ROM, also contains:
  - Sun Solaris patches
  - Avaya CMS patches
  - Avaya security script
- Avaya CMS OPENLINK Open Database Connectivity (ODBC) Driver CD-ROM (optional)
- Avaya Visual Vectors Server for CMS CD-ROM (optional)
Connectivity considerations for CMS server switch-overs

For customers who require continuous access to their CMS data, HA systems allow for the re-direction of LAN traffic related to CMS clients and other peripheral devices. Switch-over from the primary server to the backup server can be performed when the primary server experiences a major failure event and the anticipated down time is expected to be significant.

The switch-over from primary to secondary server must be done manually. The amount of effort required for the switch-over will depend on the nature of your network configuration and the type and number of CMS client and peripheral devices to be re-directed to the secondary server.

For issues and procedures associated with the switch-over from the primary to the secondary HA server, see Appendix E: What to do if an Avaya CMS server fails on page 75.

Administration operations auto-synchronized by the communication server

Some of the CMS administration changes made on either of the HA servers will be automatically synchronized on the other server via the communication server.

Call center administration changes that are auto-synchronized via the communication server include:

- Changes to VDN Skill Preferences
- VDN assignments
- Vector contents

Agent Administration changes that are auto-synchronized via the communication server include:

- Multi-agent skill change
- Change Agent skills
Administration operations requiring manual synchronization

The following operations cannot be synchronized between the two CMS servers using the backup and restore process. Instead, these operations must be performed manually on each CMS server.

Agent administration
- Agent trace administration
- Activate agent trace

Administration (other)
- Agent exceptions
- Split/Skill exceptions
- Trunk group exceptions
- VDN exceptions
- Vector exceptions

UNIX administration
- Administering passwords

Scripting and Timetables
- Create Supervisor scripts (from a supervisor login)
- Scheduling of time tables

Note:
The timetable window includes the following run options:

<table>
<thead>
<tr>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run only on this CMS server*</td>
</tr>
<tr>
<td>Run on this or another CMS server*</td>
</tr>
</tbody>
</table>

In some cases, running timetables on both servers is not desirable. For example, when a timetable specifies printing of very large reports, running the timetables on both servers would result in duplicate printings. If an administered timetable should be run only on the current server, select the Run only on this server* option. However, be aware that any timetables set up to run only on the primary server must be manually revised before they will run on the secondary server.
Primary and secondary CMS servers

System setup
- Changing the CMS state
- Data storage allocation
- External application state
- External Call History state
- Load Pseudo ACD data
- Pseudo ACD setup
- Storage intervals
- Turning data collection on and off

Maintenance
- Data summarizing
- Call center administration
- Call work codes

User permissions
- Removing CMS users

Call center administration
- VDN Call Profile
- Call Work Codes
- Split/Skill Call Profile
Administration operations synchronized by backups and restores

The following CMS administration operations can be synchronized between the two HA servers by backing up the CMS server on which the operation was performed and restoring the backup to the other server.

- Custom reports - additions or modifications to existing reports
- Avaya CMS Supervisor designer reports - additions or modifications to existing reports
- Dictionary operations, including:
  - ACDs
  - Agent groups
  - Agent string values
  - Announcements
  - AUX reason codes
  - Calculations
  - Call work codes
  - Constants
  - Custom items
  - Generic string values
  - Location IDs
  - Log in identifications
  - Log out reason codes
  - Split/skill string values
  - Split/skills
  - Trunk groups
  - Trunk string values
  - VDNs
  - Vectors
- Main menu additions (additional steps may be required)
- Timetables - additions or modifications to existing timetables
- Shortcuts - additions or modifications to existing shortcuts
- User permissions
Primary and secondary CMS servers

- ACD access
- Feature access
- Main menu addition access
- Split/skill access
- Trunk group access
- User data
- Vector access
- VDN access

Operations requiring data collection to be turned off

The ability of the CMS High Availability offer to back up, restore, and migrate data with data collection turned on significantly increases system availability. However, a limited number of operations do require data collection to be turned off while they are being performed. You must turn data collection off before performing any of the following procedures:

- Changing data storage allocation
- Restoring local system administration data
- Changing the storage intervals
- Changing the master ACD

For information on performing any of these operations, see Synchronizing after data collection is turned on/off on page 45.
User scenarios

The following user scenarios refer to the Avaya CMS servers as primary and secondary. You should perform your day-to-day administrative functions on the primary CMS server and use the secondary CMS server only when the primary is not operational. The following user scenarios describe how to perform normal CMS tasks in your High Availability configuration so that the CMS servers are kept synchronized.

This section includes the following topics:

- Modifying agent trace on page 34
- Upgrading the CMS base load on page 34
- Modifying call work codes on page 35
- Modifying agent skills on page 35
- Creating custom reports on page 35
- Creating designer reports on page 36
- Modifying the Dictionary on page 37
- Administering exceptions on page 40
- Turning External Call History on and off on page 40
- Administering forecast data storage allocation on page 41
- Administering Forecasting report data on page 41
- Synchronizing main menu additions on page 42
- Administering printers on page 42
- Scripting on page 43
- Administering shortcuts on page 43
- Setting up the split/skill call profile on page 44
- Synchronizing after data collection is turned on/off on page 45
- Running timetables only on the primary server on page 49
- Running timetables on both primary and secondary servers on page 51
- Globally editing timetables to change server ownership on page 52
- Adding or modifying users on page 54
Modifying agent trace

For maximum reliability, it is recommended that you initiate all agent traces on both the primary and secondary CMS servers. This will ensure that there is a backup for the Agent Trace information in case one of the servers goes down.

To modify agent trace:

1. Access the Agent Administration: Activate Agent Trace window on the primary CMS server.
2. Modify the trace on the primary CMS server.
3. Access the Agent Administration: Activate Agent Trace window on the secondary CMS server.
4. Modify the trace on the secondary CMS server.

Upgrading the CMS base load

When a CMS base load upgrade is performed on High Availability (HA) systems, the upgrade procedure can be performed in a manner that avoids system downtime and synchronizes data between the two HA servers.

For a description of the procedure used to perform a base load upgrade on CMS HA systems, see Appendix G: Avaya CMS base load upgrade procedure for High Availability systems on page 79.
Modifying call work codes

Call work code changes are specific to a CMS server, so any changes made on the primary CMS server must be duplicated on the secondary CMS server.

To update call work code items, do the following:

1. Perform the call work code changes you require on the primary CMS server.
2. Perform the call work code changes on the secondary CMS server.

Modifying agent skills

To change agent skills:

1. Access the Agent Administration: Change Agent Skills window on the primary CMS server.
2. Make the desired skill changes.

Note: The skill changes are written to the communication server and subsequently displayed on either CMS server.

Creating custom reports

CMS High Availability requires custom reports to exist on each CMS server in order to be run on each CMS server.

To copy custom reports from the primary server to the secondary server:

2. Back up CMS system administration data on the primary CMS server.
3. Put the secondary CMS server in single-user mode.
4. Restore CMS system administration data onto the secondary CMS server.
5. Put the secondary CMS server in multi-user mode.
Creating designer reports

CMS High Availability requires that designer reports exist on each CMS server in order to be run on each CMS server. Use one of the following three procedures to create designer reports on the secondary server.

**Method 1:**
1. Back up CMS system administration data on the primary CMS server.
2. Put the secondary CMS server in single-user mode.
3. Restore CMS system administration data onto the secondary CMS server.
4. Put the secondary CMS server in multi-user mode.

**Method 2:**
1. On the primary CMS server, copy the designer report to a file on PC or diskette. To copy a designer report from the primary server, perform the following steps:
   a. From the Supervisor console, either click on the Reports icon, or open the Commands menu and select the Reports option.
      The Select a Report window is displayed.
   b. Select the report you wish to copy from the tabbed display of lists (real-time, historical or integrated).
   c. Click the Copy button located near the bottom of the window.
      The Copy a Report screen is displayed.
   d. Select a location to which the report will be saved.
2. On the secondary CMS server, use the Avaya CMS Supervisor Copy function to add the designer report. To copy a designer report onto the secondary server, repeat steps 1a through 1c; when the Copy a Report screen is displayed, select the From a PC file to the CMS Server option.

**Method 3:**
Recreate the same designer report on the secondary CMS server.
Modifying the Dictionary

Dictionary changes are specific to a CMS, so that any changes that are made on the primary CMS server must be duplicated on the secondary CMS server.

Choose one of the following procedures:

- **Method 1:** on page 37 - Synchronizing Dictionary changes by back up and restore of ACD-specific administration data
- **Method 2:** on page 38 - Synchronizing Dictionary changes by backup and restore of specific tables
- **Method 3:** on page 39 - Administering the same Dictionary changes on both the primary and secondary CMS servers

**Method 1:**

⚠️ **Important:**

This procedure is for Dictionary operations made on a single ACD. If you will perform dictionary operations on multiple ACDs, perform the backup for all ACDs and restore for all ACDs.

1. Perform the Dictionary operation(s) on the primary CMS server.

2. On the primary CMS server, perform ACD specific administration data backup for the ACD on which you made the changes.

   **Note:**

   There are two Dictionary components that are not backed up using the ACD specific administration data backup: calculations and constants. They are backed up using CMS system administration.

3. Be sure to back up and restore CMS system administration data if you change these Dictionary components.

4. Put the secondary CMS server in single-user mode.

5. Perform ACD specific data restore for that same ACD on the secondary CMS server.

6. Return the secondary CMS server back to multi-user mode.

7. If the Visual Vectors server software is installed on the system, stop and re-start Visual Vectors on the server software in order to activate the new synonym(s) in Visual Vectors.

   To stop and restart the Visual Vectors software on the server, perform the following steps:

   a. At the command prompt, enter:

      ```bash
      setupaas
      ```
b. Select the `run_vvs` option from the displayed menu.

c. Select option 2 from the turn on/stop menu to stop the Visual Vectors server software.

d. To restart the Visual Vectors server software, select option 1.

**Method 2:**

⚠️ **Important:**

This procedure duplicates Dictionary synonyms and dictionary agent groups using the specific table backup and restore process. The specific table backup and restore process takes less time than using **Method 1:** on page 37. This process will manually synchronize the two CMS servers using the specific table backup and restore process.

1. Update Dictionary synonyms on the primary CMS server.

2. Perform specific table backup for the synonyms table on the primary CMS server. To select specific tables for backup, use the following procedure:
   a. Open the CMS main menu and select **Maintenance > Backup Data**.

   b. In the **Maintenance: Backup data** window, select the **Specific tables** option; all other data options must be de-selected.

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

   d. Move the cursor to the **Select tables** option and press **Enter** once again.

   e. Select the synonyms and then press **Enter** to access the **Action List** in the top right corner of the screen.

   f. From the action list, select the **Modify** option, then the **Run** option.

3. Perform specific table restore for the synonyms table on the secondary CMS server. To select specific tables for backup, use the following procedure:
   a. Open the CMS main menu, and select **Maintenance > Restore Data**.

   b. In the **Maintenance: Restore data** window, select the **Specific tables** option.

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

   d. Move the cursor to the **Select tables** option and press **Enter** once again.

   e. Select the synonyms and then press **Enter** to access the **Action List** in the top right corner of the screen.

   f. From the action list, select the **Modify** option, then the **Run** option.

4. If the Visual Vectors server software is installed on the system, stop and re-start Visual Vectors on the server software in order to activate the new synonym(s) in Visual Vectors. To stop and restart the Visual Vectors software on the server, perform the following steps:
a. At the command prompt, enter:

```bash
setuaas
```

b. Select the `run_vvs` option from the displayed menu.

c. Select option 2 from the turn on/stop menu to stop the Visual Vectors server software.

d. To restart the Visual Vectors server software, select option 1.

5. Update agent groups on the primary CMS server.

6. Perform specific table backup for the synonyms table (synonyms) and agent groups table (agroups) on the primary CMS server.

7. Perform specific table restore for the synonyms and agent groups table on the secondary CMS server.

8. If the Visual Vectors server software is installed on the system, stop and re-start Visual Vectors on the server software in order to activate the new synonym(s) in Visual Vectors. To stop and restart the Visual Vectors software on the server, perform the following steps:

   a. At the command prompt, enter:
   ```bash
   setuaas
   ```

   b. Select the `run_vvs` option from the displayed menu.

   c. Select option 2 from the turn on/stop menu to stop the Visual Vectors server software.

   d. To restart the Visual Vectors server software, select option 1.

**Method 3:**

Administer the same Dictionary changes on both the primary and secondary CMS servers. To ensure exact synchronization between the two servers, add the Dictionary changes in the same order on both CMS servers.
Administering exceptions

Exceptions must be administered individually on each HA server. There are three basic types of exceptions: call-based, interval-based, and CMS execution-based.

Call-based and interval-based exceptions are counted at the communication server, so the primary and secondary servers are automatically synchronized for these exception types.

CMS execution-based exceptions are counted beginning from the time that CMS is started on each HA server. Therefore, if the CMS start-up time varies between the primary and secondary server, CMS execution-based exception data will vary accordingly between the two servers.

To manually administer exceptions on a CMS server, perform the following steps:

1. From the CMS Main Menu, select the Exceptions option and press Enter.
2. Choose the Administration option from the displayed submenu and press Enter.
3. Select an Exception category from the displayed list of exception types and press Enter.

Turning External Call History on and off

CMS High Availability helps reduce the potential loss of External Call History Interface (ECHI) data sent to the ECHI server because if the primary CMS server is no longer functioning, you can start ECHI on the secondary CMS and continue to collect data.

If you do not use customized CMS reporting solutions developed by Avaya BCSI, ECHI data should be administered on only one CMS server at a time.

If you do use customized CMS reporting solutions developed by Avaya BCSI, consult with your BCSI representative for details about how to manage ECHI operations on the two servers.

If your ECHI installation is not usually running concurrently on both CMS servers, you may decide to switch External Call History data collection from the primary server to the secondary server when:

- The primary CMS server becomes inactive, goes down or CMS is turned off
- A link is down on the primary CMS server, but the link to the secondary CMS server is still up. If the link is down on the secondary as well, call the TSC for help to get the link back up (be sure to tell the TSC you have the High Availability feature).

Contact your Avaya Technical Support representative to install and authorize ECHI. In the U.S., call the National Customer Care Center Call Center Helpline at 1-800-242-2121.
Administering forecast data storage allocation

CMS High Availability permits data collection to remain on during forecasting data storage allocation.

Choose one of the following procedures:

● **Method 1:** on page 41 - Changes the forecast data storage allocation on both servers individually.
● **Method 2:** on page 41 - Copies the forecast data storage allocation from the primary server to the secondary server.

**Method 1:**

1. Change the forecast data storage allocation on the primary CMS server.
2. Change the forecast data storage allocation on the secondary CMS server.

**Method 2:**

1. Change the forecast data storage allocation on the primary CMS server.
2. Back up the ACD-specific administration data on the primary CMS server.
3. Put the secondary CMS server in single-user mode.
4. Restore the ACD-specific administration data onto the secondary CMS server.
5. Put the secondary CMS server in multi-user mode.

Administering Forecasting report data

Forecasting report data can be synchronized between HA servers by means of CMS maintenance backups and restores.

Forecasting administration data is copied to tape when you select the **ACD-specific administration** data type option in the **Maintenance: Backup Data** window.

The Forecasting report data is copied to tape when you select the **historical** data type option in the **Maintenance: Backup Data** window.
Synchronizing main menu additions

To synchronize main menu additions:

1. Create main menu additions on the primary CMS server.
2. Create main menu additions on the secondary CMS server.

Note:

If you attempt to synchronize the main menu additions by backing up from the primary CMS server and restoring on the secondary, main menu additions will appear on the secondary CMS server but the associated files will not. These files also need to be copied onto the secondary server.

Administering printers

Printers are not shared between the two CMS servers. You must administer printers separately for each CMS server. It is your choice whether or not a CMS server has a printer attached.
Scripting

This section includes the following topics:

- Interactive scripts on page 43
- Automatic scripts on page 43

Interactive scripts

Interactive scripts are specific to the Avaya CMS Supervisor PC and login where they were created. It does not matter whether the Avaya CMS Supervisor is logged into the primary CMS server or the secondary CMS server (if the primary is down) - either way, the Avaya CMS Supervisor user will be able to access their interactive scripts.

Automatic scripts

Automatic scripts are specific to each CMS server. Scripts you have created for the primary CMS server will not run on the secondary CMS server, and vice versa. Therefore, if the primary CMS server goes down and you log into the secondary CMS server, you will need to create automatic scripts for the secondary CMS server.

Administering shortcuts

To administer shortcuts in a CMS High Availability configuration:

1. Administer the shortcut on the primary CMS server.
2. Back up the CMS administration data on the primary CMS server.
3. Put the secondary CMS server in single-user mode.
4. Restore the CMS administration data onto the secondary CMS server.
5. Put the secondary CMS server in multi-user mode.
Setting up the split/skill call profile

Split/skill call profile changes are specific to each CMS server, so any changes made on the primary CMS server must be duplicated on the secondary CMS server.

**Note:**
Within the interval in which split/skill call profile changes are made, all data from the time of the profile change, and extending back to the beginning of that archive interval are lost. Therefore, it is highly recommended that:

- Split/skill call profile changes be performed at the beginning of an archive interval
- The changes be performed sequentially on both the primary and secondary servers as quickly as possible

Also, when ACD-specific administration data from the primary server is restored to the secondary server, data in the archive interval in which the restore is performed will also be lost on the secondary server. If minimization of data loss if of critical importance, after split/skill call profile changes are made on the primary server, perform a backup of both ACD-specific administration data and historical data on the primary and restore it onto the secondary server.

To update split/skill call profile items:

1. Access the **Call Center Administration: Split/Skill Call Profile Setup** screen.
2. Perform the split/skill changes you require on the primary CMS server.
3. Perform the split/skill call profile changes you require on the secondary CMS server.
Synchronizing after data collection is turned on/off

Some CMS administrative actions require CMS data collection to be turned off in order to make the required system changes. Actions that require CMS data collection to be stopped and restarted include:

- Changes to data storage allocation
- Restoring local system administration data
- Changes to storage intervals
- Changes to the master ACD

When any of the administrative changes listed above are undertaken, each CMS server should be taken down at different interval times in order to ensure that data is always being collected on the other server. The Diagram of synchronizing CMS servers after data collection is turned on/off on page 48 provides a depiction of the steps described in the Worksheet for synchronizing the CMS servers after turning data collection on/off on page 46.

This section includes the following topics:

- Worksheet for synchronizing the CMS servers after turning data collection on/off on page 46
- Diagram of synchronizing CMS servers after data collection is turned on/off on page 48
### Worksheet for synchronizing the CMS servers after turning data collection on/off

<table>
<thead>
<tr>
<th>Synchronizing the CMS servers after turning data collection on/off</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>At Time A, (see the Diagram of synchronizing CMS servers after data collection is turned on/off on page 48) tell users to log off the primary CMS server. Put the primary CMS server in single-user mode (see the appropriate Avaya CMS Administration manual for more information.)</td>
<td></td>
</tr>
<tr>
<td>Turn off data collection on the primary CMS server for all ACDs. Record the stop date and time.</td>
<td>Date/Time</td>
</tr>
<tr>
<td>Perform the desired administrative function (For example, Changing Data Storage Allocation).</td>
<td></td>
</tr>
<tr>
<td>Turn data collection back on, on the primary CMS server, and verify that all the links come back up. (See the appropriate Avaya CMS Administration manual for more information.) Record the date and time when the links come back up.</td>
<td>Date/Time</td>
</tr>
<tr>
<td>Return the primary CMS server to multi-user mode.</td>
<td></td>
</tr>
<tr>
<td>Wait until the most recent archive interval has completed. Verify that the interval has been archived on the secondary CMS server by doing the following: Using Maintenance: Archiving Status, run the report for interval archiving for all ACDs. Verify from the report that the interval archive for the interval ending at time B (see the Diagram of synchronizing CMS servers after data collection is turned on/off on page 48) has run.</td>
<td></td>
</tr>
<tr>
<td>At Time B’ (see the Diagram of synchronizing CMS servers after data collection is turned on/off on page 48), perform an incremental historical backup of all ACDs on the secondary CMS server.</td>
<td></td>
</tr>
<tr>
<td>Restore the historical data of specific start/stop dates/times of all ACDs to the primary CMS server. Use the time at the beginning of the interval during which the interruption occurred on the primary CMS server (for example, if the interval is 30 minutes long and occurs on the hour, and the link went down at 5:13, enter 5:00, not 5:13 as the start time.) Also enter the stop time for the end of the interval during which the interruption occurred (for example, if the link went down at 5:13 and came back up at 5:19, enter 5:29 as the stop time).</td>
<td></td>
</tr>
<tr>
<td>Put the secondary CMS server in single-user mode.</td>
<td></td>
</tr>
<tr>
<td>Turn data collection off on the secondary CMS server. Record the date and time.</td>
<td>Date/Time</td>
</tr>
<tr>
<td>Perform the same administrative function you did above for the primary CMS server on the secondary CMS server.</td>
<td></td>
</tr>
</tbody>
</table>
Synchronizing after data collection is turned on/off

<table>
<thead>
<tr>
<th>Synchronizing the CMS servers after turning data collection on/off</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn data collection “on” on the secondary CMS server. Record the date and time when the links come back up.</td>
<td>Date/Time</td>
</tr>
</tbody>
</table>

Put the secondary CMS server in multi-user mode.

After the ACD links come back up, wait for the end of that interval.

At Time C (see the Diagram of synchronizing CMS servers after data collection is turned on/off on page 48), verify that the interval you are backing up has been archived on the secondary CMS server.

At Time C’ (see the Diagram of synchronizing CMS servers after data collection is turned on/off on page 48), perform an incremental backup of all ACDs on the primary CMS server.

**Note:**
If a daily/weekly/monthly archive occurred before you synchronized data at time B’ or time C’, then after you synchronize the data (at time B or C) you must run the appropriate daily/weekly/monthly archive. Using System Setup…Data summarizing, rerun the daily/weekly/monthly archive to recreate the data.

Restore the Historical data of specific start/stop and dates/times of all ACDs to the secondary CMS server. For example, if the interruption on the secondary CMS server occurred at 5:35 and ended at 5:42, enter 5:30 for the start time and 5:59 for the stop time.

Wait until the most recent interval during which the link came back up has been archived before performing the backup and restore process. In the scenario described above, the link was down for only a single interval for both the primary and secondary CMS servers. If the link is down for multiple intervals, wait until the link has come back up before performing the backup and restore process.
Diagram of synchronizing CMS servers after data collection is turned on/off

**Synchronizing CMS Servers**  
after Data Collection Is Turned On/Off

<table>
<thead>
<tr>
<th>Secondary CMS server</th>
<th>Primary CMS server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Time A (Interval A begins)</td>
</tr>
<tr>
<td></td>
<td>Link up</td>
</tr>
<tr>
<td></td>
<td>Link up</td>
</tr>
<tr>
<td></td>
<td>Turn off data collection</td>
</tr>
<tr>
<td></td>
<td>Link down (perform admin)</td>
</tr>
<tr>
<td></td>
<td>Turn on data collection</td>
</tr>
<tr>
<td></td>
<td>Link back up</td>
</tr>
<tr>
<td>synchronize</td>
<td>Time B (Interval B begins)</td>
</tr>
<tr>
<td></td>
<td>Time B’</td>
</tr>
<tr>
<td></td>
<td>Link up</td>
</tr>
<tr>
<td></td>
<td>Link back up</td>
</tr>
<tr>
<td></td>
<td>Link up</td>
</tr>
<tr>
<td></td>
<td>Link back up</td>
</tr>
<tr>
<td>synchronize</td>
<td>Time C (Interval C begins)</td>
</tr>
<tr>
<td></td>
<td>Time C’</td>
</tr>
<tr>
<td></td>
<td>Link up</td>
</tr>
<tr>
<td></td>
<td>Link down</td>
</tr>
</tbody>
</table>

**Note:** If a daily/weekly/monthly archive occurred before you synchronized data at time B’ or time C’, then after you synchronize the data (at time B or C) you must run the appropriate daily/weekly/monthly archive. Using **System Setup…Data summarizing**, rerun the daily/weekly/monthly archive to recreate the data.

Note from the graphic at what point in time events occur.

---

48 Avaya CMS High Availability User Guide
Running timetables only on the primary server

In most cases, you will want to run a timetable from only the primary CMS server.

To run a timetable from only the primary CMS server:

1. Create a timetable on the primary CMS server.
2. Enter the timetable screen on the primary CMS server.
   
   At the bottom of the timetable screen you will see the following:

   This timetable will run on this or another CMS server
   < > Run only on this CMS server
   <X> Run on this or another CMS server

   The default is for the timetable to run on the primary or another CMS server. However, if you back up the timetable and restore it to the secondary CMS server with the default setting, the system will run the identical timetable on the secondary CMS server as well, causing duplication.

3. Change the setting to Run only on this CMS server.
   
   The select option will appear as:

   This timetable will run on this or another CMS server
   <X> Run only on this CMS server
   < > Run on this or another CMS server

4. Back up the data on the primary CMS server by selecting the CMS system administration data option in the Maintenance:Backup data window.
5. On the secondary server, change CMS to single-user mode.
6. Restore the data onto the secondary CMS server using Maintenance Restore.
7. Change CMS back to multi-user mode on the secondary server.
8. On the secondary CMS server, display the timetable you created.
   
   At the bottom of the timetable screen you will see the following:

   This timetable will not run on this CMS server
   < > Run only on this CMS server
   < > Run on this or another CMS server
9. Accept the default setting.

As a result, a copy of the timetable exists on the secondary CMS server but the timetable will run only from the primary CMS server.

**Note:**
- If you wish to run the timetable from the secondary CMS server, you may check either box.
- Then press **Enter** to access the action list in the upper right corner of the window, select the **Modify** option and press **Enter** once again. The timetable now runs on both the primary and secondary CMS servers.
Running timetables on both primary and secondary servers

There may be instances when you want to run a timetable from both the primary and secondary CMS servers. For example, since the maintenance error log report is specific to a CMS server, you may want the timetable to run and produce a maintenance error log report for each CMS server.

If you wish to run a timetable from both the primary and secondary CMS servers:

1. Create a timetable on the primary CMS server.
2. On the primary CMS server, enter the timetable screen by accepting the default selection:

   This timetable will run only on this CMS server
   < > Run only on this CMS server
   <X> Run on this or another CMS server

3. Use the Add command to add the timetable.
4. After you have created all the tasks for the timetable and use the Stop function to end the task creation, the timetable screen now has the following displayed (in addition to all timetable information):

   This timetable will run on this or another CMS server
   < > Run only on this CMS server
   <X> Run on this or another CMS server

   The timetable will now run as scheduled on the primary CMS server
5. Back up the data on the primary CMS server by using Maintenance > Back Up Data option.
6. On the secondary server, change CMS to single-user mode.
7. Restore the data on the secondary CMS server using the Maintenance Restore option.
8. Change CMS back to multi-user mode on the secondary server.

   The timetable you restored to the secondary CMS server is automatically scheduled to run on the secondary CMS server as well as on the primary CMS server.

If you log on to the secondary CMS server and look at the timetable, you will see the following lines at the bottom of the timetable screen:

   This timetable will run on this or another CMS server
   < > Run only on this CMS server
   <X> Run on this or another CMS server
Globally editing timetables to change server ownership

Use this procedure if the primary CMS server fails and you would like to globally edit timetables to ensure that they will all run on the secondary server.

The following procedure assumes that:

- Timetables exist on both your primary and secondary CMS servers
- The timetables are owned by more than one user

⚠️ Important:
If you make administration changes on the secondary server during the interval in which the primary server is not operational, and you wish to transfer those changes to the primary server after it is restored, you must restore timetables to their normal run state on the two HA servers (see steps 8 through 13, below). If the primary server outage is not anticipated to be extensive in duration, it is recommended that no administration changes be made on the secondary server while the primary server is out of service.

1. Log into the secondary CMS server as “cms”, so you have permission to globally edit all users’ timetables.
2. Enter the timetable screen.
3. Clear the timetable screen (Ctrl+Z) and use the List all function to determine all users who own timetables, and record their user IDs.
4. Enter an individual user ID.
5. Using the Global edit function, enter the Global edit screen for that user ID.

You will see the following:

```
For all timetables owned by User ID XXXXXX
Select one:
< > Run timetables only on this CMS server
< > Run timetables on this or another CMS server
```

where XXXXXX is the user ID.

6. Select one of the options listed in Step 5. Either option will immediately schedule all timetables for that user ID.
Important:
Once the global edit has been performed on the secondary CMS server, it cannot be “undone”. The only way to “undo” a global edit to these timetables is to once again restore the timetables from the primary CMS server to the secondary CMS server.

7. When the primary server is returned to service, choose between the following options:

- If you have not made any CMS administration changes on the secondary server (including timetable modifications or revisions) that you wish to transfer to the primary server, return the timetables on the secondary server to their normal run state by using the most recent CMS administration backup created on the primary server and restoring it onto the secondary server. **You can disregard the remaining steps.**

- If you have made any CMS administration changes on the secondary server and wish to transfer them to the primary server after it is brought back to service, continue with the additional steps listed below to return all timetables to their normal run state on the two HA servers.

8. Perform a CMS system administration backup of the secondary CMS server.

9. On the primary server, change CMS to single-user mode.

10. Restore system administration data to the primary CMS.

11. Return CMS to multi-user mode on the primary server.

   Now, all timetables on the primary CMS server are duplicates of the timetables on the secondary. However, since the “Run timetables only on this CMS server” global edit on all timetables occurred on the secondary CMS server, none of the timetables will run on the primary server.

12. Repeat Steps 1 through 6 of this procedure on the primary server to globally edit the timetables to run only on the CMS server.

13. Perform a CMS system administration backup on the primary server and restore it onto the secondary server.
Adding or modifying users

To administer a new user on the CMS High Availability system:

1. Add the new user on the primary CMS server
2. Restore the data to the secondary CMS server
3. Add users and user permissions on the primary CMS server.
   For more information, see the section about administering user permissions in the appropriate CMS administration guide for your CMS release.
4. Perform a maintenance backup of CMS system administration data and ACD-specific administration data on the primary CMS server.
   For more information, see the section about performing a maintenance backup in the appropriate CMS administration guide for your CMS release.
5. Log in to the secondary CMS server and change to single-user mode.
6. Perform a maintenance restore of CMS system administration data and ACD-specific administration data on the secondary CMS server for all ACDs.
   For more information, see the section about restoring data in the appropriate CMS administration guide for your CMS release.
7. Change the secondary server back to multi-user mode.
8. Log off the secondary server.

Note:

Maintenance restore of CMS system administration data replaces the user data and generates a UNIX login and a user directory for logins that are on the backup tape. Maintenance restore of ACD-specific administration data replaces the user permissions. CMS user passwords must be administered separately on each CMS server. For more information, see Setting user passwords on page 55.

Removing users

To remove CMS users:

1. Delete the user(s) from the primary CMS server.
2. Delete the same user(s) from the secondary CMS server.
Setting user passwords

This section describes how to administer CMS user passwords on an HA server. The passwords must be administered separately on each server.

To set user passwords:

1. Log in to CMS.
   The CMS main menu is displayed.
2. At the CMS main menu, press F3 to select the COMMANDS option.
   The commands options window is displayed.
3. Use the cursor keys to select the Unix(r) system option and press Enter.
   A terminal window is displayed.
4. At the command prompt, enter:
   \texttt{su - cms}
5. Log in as root and enter:
   \texttt{passwd userid}
   where \textit{userid} is the ID for a CMS user
6. At the prompt, enter the password for the CMS user. This password should be identical to the password administered on the other HA server.
7. Repeat Steps 5 and 6 for each CMS user on the system.
8. After you have administered user passwords, enter:
   \texttt{exit}
   The system returns to the CMS main menu.
Administering the VDN call profile

VDN call profile administration changes are specific to a CMS server, so any changes made on the primary CMS server must be duplicated on the secondary. Within the interval in which VDN call profile administration changes are made, all data from the time of the profile change and extending back to the beginning of that archive interval are lost. Therefore, it is highly recommended that:

- VDN call profile changes be performed at the beginning of an archive interval
- the changes be performed sequentially on both the primary and secondary server as quickly as possible

Also, when ACD-specific administration data from the primary server is restored to the secondary server, data in the archive interval in which the restore is performed will be lost on the secondary server. Therefore, if minimization of data loss is of critical importance, after VDN call profile changes are made on the primary server, perform a backup of both ACD-specific administration data and historical data on the primary and restore it onto the secondary server.

To update VDN call profile administration items:

1. Access the Call Center Administration: VDN Call Profile Setup screen.
2. On the primary CMS server, perform the VDN call profile administration changes you require.
3. Perform the VDN call profile changes you require on the secondary CMS server.
Administering Avaya Visual Vectors

Avaya recommends that you administer Visual Vectors only from the primary CMS server. By administering Visual Vectors only from the primary CMS server, you will always know the most recent Visual Vectors information resides on the primary CMS server. This will greatly reduce the risk of losing Visual Vectors comments.

To change vectors:

1. Launch Visual Vectors and connect to the primary CMS server.
2. Make vector changes.
3. Save vector changes.
4. Log in to the primary CMS server and back up the Avaya Visual Vectors server data via the setupaas menu.
5. Log in to the secondary CMS server and restore the Avaya Visual Vectors server data via the setupaas menu.

Note:

Vector changes (except vector comments) are written to the communication server and subsequently reflected on both CMS servers regardless of which server (primary or secondary) is in use.

Backing up and restoring Visual Vectors server data must be performed after each session where vector changes are made or you risk losing Visual Vector comments.
User scenarios
High Availability backup and restore strategy

High Availability configurations use the same tape backup procedures used by standard Avaya CMS configurations. LAN backup is not supported on High Availability configurations. For a description of the normal CMS server backup/restore process and schedule, see Appendix A: CMS backups and restores on page 63.

A set of dedicated synchronization tapes capable of holding one backup of each CMS server should also be maintained. Whenever you make a change to a CMS server that you would like to back up and restore to the other CMS server, perform a manual backup using the dedicated synchronization tapes.

This section includes the following topics:

- Synchronizing after an unscheduled outage of the primary CMS server on page 60
- Synchronizing after an unscheduled outage of the secondary CMS server on page 61
Synchronizing after an unscheduled outage of the primary CMS server

This procedure presumes users are temporarily logged into the secondary CMS server because the primary CMS server was not operational.

To synchronize the servers after an unscheduled outage of the primary server:

1. After the primary CMS server is back up and running, note the date and time, and perform a full maintenance backup of the secondary CMS server.

2. Put the primary CMS server in single-user mode.

3. If you made administration changes on the secondary CMS server while the primary was down, restore both the ACD-specific and CMS administration data from the secondary CMS server full maintenance backup to the primary CMS server.

4. Put the primary CMS server in multi-user mode.

5. Wait for an interval to complete and be archived.

6. Restore the specific start/stop and time/date historical data to the primary CMS server to recover the needed data.

7. Tell users to log off the secondary CMS server and log back into the primary CMS server.
Synchronizing after an unscheduled outage of the secondary CMS server

To synchronize the servers after an unscheduled outage of the secondary server:

1. After the secondary CMS server is back up and running, do a full maintenance backup of the primary CMS server.

2. Put the secondary CMS server in single-user mode. For more information, see the appropriate Avaya Call Management System administration document for your CMS release.

3. If you made administration changes on the primary CMS server while the secondary was down, restore both the ACD-specific and CMS Administration data from the primary CMS server full maintenance backup to the secondary CMS server.

4. Put the secondary CMS server in multi-user mode.

5. Restore the specific start/stop and time/date historical data to the secondary CMS server to recover the needed data.
High Availability backup and restore strategy
Appendix A: CMS backups and restores

This section includes the following topics:

- Backup and restore procedures on page 63
- Avaya CMS backup strategy on page 64

Backup and restore procedures

The tape backup and restore procedures are identical to those used for non-high availability configurations. LAN backup is not supported on High Availability configurations. Because you are working with two servers, be sure to label your backup tapes as primary and secondary.

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.

Related topics
For the maintenance or CMSADM backup procedures, see the section about maintaining a CMS data backup in the appropriate CMS administration guide for your CMS release.

For the LAN backup procedure, see the appropriate Avaya CMS LAN backup user guide for your CMS release.
Avaya CMS backup strategy

Since new data is written each day, the data should be backed up regularly. Use a backup strategy appropriate to your call center. Managing the tapes (storage, security, and labeling) is key to ensuring that if a restore is needed, you can do it quickly and accurately. Keep enough tapes on hand to rotate the tapes so that several tapes are available at all times. For example, you can keep two weeks worth of tapes in stock and recycle them weekly (for an environment in which you do daily backups, you use a new tape each day of the week and repeat each weekly sequence).

Perform a full maintenance backup after the Avaya CMS software has been initially installed and tested.

You must do a full backup before doing the first incremental backup.

A full maintenance backup should be performed nightly, using multiple backup tapes in a regular rotation scheme.

A CMSADM backup should be performed at least one time per month.

Labeling the backup volume

After a successful backup, the computer automatically labels your backup volumes. Avaya CMS provides the backup information in the final Acknowledgment window or, if the backup was scheduled on a timetable, in the maintenance error log.

Backup tapes can wear out. Be sure to refresh your supply of backup tapes at appropriate intervals. For more information, see the documentation that came with your backup tapes. Note that the machines need to have matching tape drives and the appropriate tapes for those drives.

You should have the appropriate number of tapes for the backup. When you run a manual backup (not from a timetable), you get an acknowledgment in the Back Up Data window that tells you the number of tapes needed for a full backup. (Incremental backups should fit on one tape so no estimate is needed.)

Backup information format

0001CMS-NNNNNN-NN-LLLL-NN-L-NN
000211111I
00031234567
# How to interpret backup information

Use this table to decode backup information.

<table>
<thead>
<tr>
<th>Part #</th>
<th>Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CMS</td>
<td>System name</td>
</tr>
<tr>
<td>2</td>
<td>NNNNNNN</td>
<td>Year, month and day of the backup, in the form yymmdd</td>
</tr>
<tr>
<td>3</td>
<td>NN</td>
<td>Number of backups for this day</td>
</tr>
</tbody>
</table>
| 4      | LLLL     | Type of data backed up: A for both ACD-specific administration data and historical data C for custom data H for historical data L for local system administration data M for ACD-specific administration data S for CMS system data X for no backup  
In the 1st position, an “L” appears if local System Administration data was backed up, or an “X” displays if no local System Administration data was backed up.  
In the 2nd position, an “S” appears if system data was backed up or an “X” displays if system data was not backed up.  
In the 3rd position, an “H”, “M”, “A”, or “X” displays.  
In the 4th position, a “C” or “X” displays.  
Any combination of letters identifying the type of backup may display. |
| 5      | NN       | Number of the ACD (00 means the All ACDs option was selected on the Back Up window)                                                        |
| 6      | L        | Backup mode (F for Full, I for Incremental)                                                                                               |
| 7      | NN       | The tape number in the backup series (for this backup only)                                                                               |
CMS backups and restores
Appendix B: Items excluded from a CMSADM backup

A CMSADM backup copies all system directories and files, with a few exceptions. Depending on your CMS load, some of the files that may be excluded are:

- any swap devices (such as those displayed with "swap -l")
- /proc
- /cdrom
- /
- /tmp
- /core
- /vol
- /floppy
- /xfn
- /usr/lib/cms/Aname
- /usr/lib/cms/Pname
- /usr/lib/cms/Sname
- /cms/cmstables
- /cms/db/inf/cms.dbs
- /cms/db/gem/c_custom
- /cms/db/gem/h_custom
- /cms/db/gem/r_custom
- /cms/db/journal/shortcut
- /cms/db/journal/timetable
- /cms/pbx/master
- /cms/pbx/sim_pbx
- /cms/tmp
- /dev/fd
Items excluded from a CMSADM backup

- /var/tmp
- /dump/tmp
- /etc/saf/zsmon/_pmpipe
- /etc/saf/zsmon/_pid
- /etc/saf/_sacpipe
- /etc/saf/_cmdpipe
- /etc/mnttab
- /etc/initpipe
- /etc/syslog.pid
- /var/spool/lp/temp
- /var/spool/lp/tmp
- /var/spool/lp/requests
- /etc/nologin
- /usr/dbtemp
- /etc/.name_service_door"
Appendix C: Items backed up during a full maintenance backup

Note that a pathname with one or more slashes ("/") indicates a UNIX file or directory. A pathname with no slashes indicates an Informix table.

Local system administration
- dcadmin
- dcalloc
- print_adm
- /usr/lib/pbx/Aname
- /usr/lib/pbx/Pname
- /usr/lib/pbx/Sname
- fullex
- H_hostname

CMS system administration data
- custobjects
- /cms/db/ext
- /cms/db/gem/c_custom
- /cms/db/gem/h_custom
- /cms/db/gem/r_custom
- dbitems
- cmstbls
- features
- h_custom
- main_menu
- menu_add
- menu
Items backed up during a full maintenance backup

- /cms/pbx/master
- /cms/pbx/sim_pbx
- r_custom
- scwininfo
- sys_info
- user_colors
- user_defval
- users
- /cms/cow/reports/designer
- /cms/db/journal/shortcut
- /cms/db/journal/timetable
- ttsched
- ttstasks
- ttsc

ACD administration data

- aar_agents
- acd_shifts
- acds
- ag_ex_adm
- agroups
- arch_stat
- dbstatus
- f_cdayconf (forecasting)
- f_chpap (forecasting)
- f_chprof (forecasting)
- f_cstap (forecasting)
- f_cstprof (forecasting)
- f_dataarch (forecasting)
- f_spdays (forecasting)
- f_status (forecasting)
- f_tkgpprof (forecasting)
- sp_ex_adm
- split_pro
- splits
- synonyms
- tg_ex_adm
- tgroups
- vdn_pro
- vdn_x_adm
- vdns
- vec_x_adm
- vectors

**Historical data**
- ag_actv
- agex
- call_rec
- haglog
- linkex
- mctex
- spex
- tgex
- vdnex
- vecex
- d_secs
- dagent
- dcwc
- dsplit
- dtkgrp
- dtrunk
- dvdn
- dvector
- f_cday (forecasting)
- f_cdayrep (forecasting)
- f_dsplt (forecasting)
Items backed up during a full maintenance backup

- f_dtkggrp (forecasting)
- f_ispday (forecasting)
- f_isplit (forecasting)
- f_itkgrp (forecasting)
- hagent
- hcwc
- hsplit
- htkgrp
- htrunk
- hvdn
- hvector
- m_secs
- magent
- mcwc
- msplit
- mtkgrp
- mtrunk
- mvdn
- mvector
- w_secs
- wagent
- wcwc
- wsplit
- wtkgrp
- wtrunk
- wvdn
- wvector
Appendix D: Restore characteristics of different data types

Local system administration data
This is data specific to the particular Avaya CMS server on which it was administered. This data can be restored only onto the server from which it was copied.

CMS system administration data
Some administrative data is not ACD-specific, such as:

- User data
- Timetables
- Custom reports

When you restore this data, the information in the tables are deleted. After the tables are deleted, they are then restored from the backup tape.

ACD-specific administration data
Some data is specific to a particular ACD, such as:

- Exceptions administration data
- Dictionary items
- Split/skill call profiles

When you restore this data and copy it over existing tables, the existing tables are deleted, and the new tables are copied onto the system from the backup.

Historical data
Historical data includes interval, daily, weekly, and monthly archived call data. In addition, historical data also includes event data, which consists of:

- Agent login/logout data
- Agent trace data
- Exceptions data
- Internal call record data
When historical data is restored from a maintenance backup tape, the restore program creates a restore range, which is based on the available data actually found on the backup tape. The restore range is not necessarily identical to the start and stop times you specify in the restore window. For instance, disparities between specified and actual restore ranges can occur when the stop time specified in the restore exceeds the end time for the last data rows for a given table copied to the backup.

After the restore range is calculated by the program, any existing data rows in the current table that fall within the calculated restore range are deleted. The restore program then copies in the new data to the table, which replaces all of the previously deleted rows, as well as any new data rows that may have been included in the actual restore range.
Appendix E: What to do if an Avaya CMS server fails

This section includes the following topics:
- Primary CMS server on page 75
- Secondary CMS server on page 76
- Both CMS servers on page 76

Primary CMS server

If one or more links to the primary CMS server goes down:

1. Log into your secondary CMS server and verify status of the link(s) on it.
2. If the links are up on the secondary CMS server, inform your users that they should log off of the primary and log onto the secondary.
3. If you have ECH, turn it “on” on the secondary CMS server and off on the primary CMS server.
4. Call the Helpline and inform them you are a High Availability configuration and that one or more links are down on the primary CMS server.

If the primary CMS server is exhibiting problems (for example, users are unable to log in, reports do not run, missing archive intervals):

1. Instruct users to log off of the primary and log on to the secondary CMS server.
2. Call the Helpline and inform them you are a High Availability configuration and describe the problem.

If the primary CMS server goes down, do the following:

1. Verify that your secondary CMS server is up and the link(s) are up.
2. Inform your users that they should log into the secondary CMS server.
3. Call the Helpline and inform them you are a High Availability configuration and tell them the primary CMS server is down.
What to do if an Avaya CMS server fails

Secondary CMS server

If the secondary CMS server goes down, do the following:

1. Verify that your primary CMS server is up and the link(s) are up.
2. Call the Helpline and inform them you are a High Availability configuration and tell them the secondary CMS server is down.

Both CMS servers

Call the Helpline, inform them you are a High Availability configuration and tell them links to both CMS servers are down. High Availability is not a Disaster Recovery system, so if data is lost on both systems, you have lost data for the interval(s) in question.
Appendix F: Frequently asked questions

- What is the purpose of the Avaya CMS High Availability offer?
  The purpose of the CMS High Availability offer is to ensure data availability between the communication server and the CMS system by connecting two CMS servers at one site to a single communication server, thereby eliminating the traditional single point of failure between the CMS and the communication server.

- Are the primary and secondary CMS servers aware of each other?
  No. Both CMS servers collect data from the communication server, but they operate completely independently and are not even aware of each other.

- What is the purpose of the dual ACD link?
  The dual ACD link feature addresses ACD link failures and builds on the increased ACD link reliability provided by TCP/IP.

- Does each CMS server collect the same data?
  Yes. Both CMS servers collect identical real-time, historical, and call record data.

- When I attempt to simultaneously view Real Time Reports on both of the HA servers, why don’t the reports match precisely?
  There are several reasons why this can occur. Real Time reports are pushed to the client at specified intervals - the “refresh rate”. Most likely, you did not start the reports at exactly the same time, so there is a slight lag in data reporting associated with the staggered refresh rates between the two servers. In addition, it is also possible that different refresh rates have been set for the two servers.

- How do I know when I should perform a server switch-over from the primary to the secondary HA server?
  Server switch-overs are not recommended for system outages of relatively brief duration. However, it is the responsibility of each CMS customer to establish their own criteria as to exactly what constitutes an unacceptable amount of time during which call data remains unavailable for analysis and review.
Frequently asked questions
Appendix G: Avaya CMS base load upgrade procedure for High Availability systems

When an Avaya CMS base load upgrade is performed on High Availability (HA) systems, the upgrade procedure can be performed in a manner that avoids system downtime and synchronizes data between the two HA servers.

For a complete listing of the most current CMS base load upgrade procedures, refer to the load-specific documentation that shipped with the CMS base load upgrade CD-ROM.
Avaya CMS base load upgrade procedure for High Availability systems
Index

A
ACD
  call processing software ........................................... 19
  link failures ......................................................... 21
administrating
  exceptions ............................................................. 40
forecast data storage allocation ........................................ 41
Forecasting ............................................................... 41
printers ................................................................. 42
shortcuts ................................................................. 43
VDN call profile ....................................................... 56
Visual Vectors ........................................................... 57
agent skills, changing .................................................. 35
agent trace, modifying ............................................... 34
automatic scripts ....................................................... 43
automatically synchronized operations ................................ 28

B
backup
  HA ........................................................................... 59
backup and restore procedures .......................................... 63
base load upgrade ....................................................... 79

C
callwork codes, updating ................................................ 35
CMS
  base load upgrade ....................................................... 79
  required software ....................................................... 26
  software failures ....................................................... 21
CMS server
  hardware failures ....................................................... 21
  maintenance ............................................................. 21, 25
  manual synchronization ............................................... 20
  primary ................................................................. 23
  secondary ............................................................. 23
  upgrades .............................................................. 22
CMS server fails .......................................................... 75
CMS users
  adding or modifying ................................................... 54
  removing ............................................................... 54
  setting user passwords ............................................... 55
CMSADM backup .................................................................. 67
  connectivity switch-overs ............................................. 28
custom reports .............................................................. 35

data availability ................................................................ 21
data collection
  synchronizing CMS servers ......................................... 45, 46
data types
  restore characteristics ................................................. 73
designer reports ............................................................. 36
Dictionary ........................................................................ 37
dual ACD links ............................................................. 19

data availability ................................................................ 21
data collection
  synchronizing CMS servers ......................................... 45, 46
data types
  restore characteristics ................................................. 73
designer reports ............................................................. 36
Dictionary ........................................................................ 37
dual ACD links ............................................................. 19

data availability ................................................................ 21
data collection
  synchronizing CMS servers ......................................... 45, 46
data types
  restore characteristics ................................................. 73
designer reports ............................................................. 36
Dictionary ........................................................................ 37
dual ACD links ............................................................. 19

data availability ................................................................ 21
data collection
  synchronizing CMS servers ......................................... 45, 46
data types
  restore characteristics ................................................. 73
designer reports ............................................................. 36
Dictionary ........................................................................ 37
dual ACD links ............................................................. 19

data availability ................................................................ 21
data collection
  synchronizing CMS servers ......................................... 45, 46
data types
  restore characteristics ................................................. 73
designer reports ............................................................. 36
Dictionary ........................................................................ 37
dual ACD links ............................................................. 19

data availability ................................................................ 21
data collection
  synchronizing CMS servers ......................................... 45, 46
data types
  restore characteristics ................................................. 73
designer reports ............................................................. 36
Dictionary ........................................................................ 37
dual ACD links ............................................................. 19

data availability ................................................................ 21
data collection
  synchronizing CMS servers ......................................... 45, 46
data types
  restore characteristics ................................................. 73
designer reports ............................................................. 36
Dictionary ........................................................................ 37
dual ACD links ............................................................. 19

data availability ................................................................ 21
data collection
  synchronizing CMS servers ......................................... 45, 46
data types
  restore characteristics ................................................. 73
designer reports ............................................................. 36
Dictionary ........................................................................ 37
dual ACD links ............................................................. 19

E
enhancements .................................................................... 20
exceptions ........................................................................ 40
External Call History
  turning on and off ....................................................... 40

F
forecast data storage allocation .......................................... 41
Forecasting ........................................................................ 41
frequently asked questions ................................................ 77
full maintenance backup
  items backed up .......................................................... 69

globally editing timetables ................................................ 52

H
Hardware
  failures ....................................................................... 21
helplines ........................................................................ 15
High Availability, defined ............................................... 17

I
interactive scripts ........................................................... 43
| M | manually synchronized operations | 29 |
|   | manually synchronizing servers | 20 |
| O | operations |
|   | automatically synchronized | 28 |
|   | manually synchronized | 29 |
|   | requiring data collection to be turned off | 32 |
|   | synchronized by backups and restores | 31 |
| P | primary CMS server | 23 |
|   | unscheduled outage synchronizing | 60 |
|   | printers | 42 |
| R | R3V8 and later enhancements | 20 |
|   | recovery kit | 26 |
|   | reports |
|   | custom | 35 |
|   | designer | 36 |
|   | restore characteristics |
|   | data types | 73 |
|   | running |
|   | timetables on both primary and secondary servers | 51 |
|   | timetables only on the primary server | 49 |
| S | scripting | 43 |
|   | secondary CMS server | 23 |
|   | unscheduled outage synchronizing | 61 |
|   | set up |
|   | split/skill call profile | 44 |
|   | shortcuts | 43 |
|   | software |
|   | failures | 21 |
|   | shipped with CMS | 26 |
|   | split/skill call profile | 44 |
|   | synchronization |
|   | data | 23 |
|   | main menu additions | 42 |
|   | synchronizing CMS servers | 45 |
| T | timetables | 52 |
|   | running on both primary and secondary servers | 51 |
|   | running only on the primary server | 49 |
|   | turning External Call History on and off | 40 |
| U | updating |
|   | agent skills | 35 |
|   | call work codes | 35 |
|   | upgrades |
|   | base load | 34, 79 |
| V | VDN call profile administration | 56 |
|   | Visual Vectors |
|   | administering | 57 |