Avaya™ CMS

R3V11

High Availability User Guide

585-215-714
Comcode 700203318
Issue 1.0
May 2002
Compas ID 89410

© 2002, Avaya Inc.
All Rights Reserved

Notice

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

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you *suspect that you are being victimized* by toll fraud and you need technical support or assistance, call Technical Service Center Toll Fraud Intervention Hotline at +1 800 643 2353.

Providing Telecommunications Security

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

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

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

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

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

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

Your Responsibility for Your Company's Telecommunications Security

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

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

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

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

Federal Communications Commission Statement

Part 15: Class A Statement. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

European Union Declaration of Conformity

Avaya Business Communications Systems declares that equipment specified in this document conforms to the referenced European Union (EU) Directives and Harmonized Standards listed below:

EMC Directive 89/336/EEC

Low Voltage Directive 73/23/EEC

CE The "CE" mark affixed to the equipment means that it conforms to the above Directives.

Trademarks

MultiVantage is a trademark of Avaya, Inc.

DEFINITY is a registered trademark of Avaya, Inc.

Enterprise, Solaris, SPARCserver, Sun, SunSwift, Sun Blade 100, and Ultra are trademarks or registered trademarks of Sun Microsystems, Inc.

INFORMIX is a registered trademark of Informix Software, Inc.

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

Ordering Information

Call: US Voice: 1 800 457 1235
US Fax: 1 800 457 1764
non-US Voice: +1 410 568 3680
non-US Fax: +1 410 891 0207

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA

Order: Document No. 585-215-714, Issue 1.0
Comcode 700203318, May 2002

You can be placed on a Standing Order list for this and other documents you may need. Standing Order will enable you to automatically receive updated versions of individual documents or document sets, billed to account information that you provide. For more information on Standing Orders, or to be put on a list to receive future issues of this document, please contact the Avaya Publications Center.

Avaya National Customer Care Center

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.

Avaya Web Page

http://www.avaya.com

Acknowledgment

This document was written by the CRM Development group.

Avaya CMS R3V11
High Availability User Guide

Contents

Preface

Overview . . . 7
Scope . . . 7
Contents . . . 7
Reasons for re-issue . . . 8
Conventions . . . 8
Related documents . . . 9
CMS software documents . . . 9
Upgrade documents . . . 10
Hardware documents . . . 12
Switch documents . . . 12
Administration documents . . . 13
Other documents . . . 13
Documentation Web sites . . . 14
If you have a problem . . . 15

Introduction

Overview . . . 17
HA server switch-over after a failure event . . . 18
Dual ACD links . . . 19
Hardware platforms . . . 20
CMS feature enhancements . . . 21
Increased data availability . . . 22

Primary and secondary CMS servers

Overview . . . 25
CMS HA server maintenance . . . 27
CMS recovery kit . . . 28
Purpose . . . 28
Recovery kit contents . . . 28
Recovery kit software components . . . 29
Connectivity considerations for CMS server switch-overs . . . 30

Admin operations auto-synchronized by the switch . . . 31
Admin operations requiring manual synchronization . . . 32
Admin operations synchronized by backups and restores . . . 34
Operations requiring data collection to be turned off . . . 36

User scenarios

Overview . . . 37
Modifying Agent Trace . . . 37
Upgrading the CMS base load . . . 38
Changing call work codes . . . 38
Changing agent skills . . . 39
Creating custom reports . . . 39
Creating designer reports . . . 40
Changing the dictionary . . . 41
Method 1 - Synchronizing dictionary changes by back up and restore of ACD-specific administration data . . . 41
Method 2 - Synchronizing dictionary changes by backup and restore of specific tables . . . 42
Method 3 - Administering the same dictionary changes on both the primary and secondary CMS servers . . . 43
Administering exceptions . . . 44
Turning on and off External Call History . . . 45
Administering forecast data storage allocation . . . 46
Method 1 . . . 46
Method 2 . . . 46
Administering forecasting report data . . . 47
Synchronizing main menu additions . . . 47
Administrating printers . . . 47
Scripting . . . 48
Interactive scripts . . . 48
Automatic scripts . . . 48
Administering shortcuts . . . 49
Setting up the split/skill call profile . . . 49
Synchronizing after data collection is turned On/Off . . . 50
Running timetables only on the primary server . . . 54
Running timetables on both primary and secondary servers . . . 56
Globally editing to timetables to change server ownership . . . 58
Adding or modifying users . . . 60
Removing users . . . 61
Users - setting user passwords . . . 61
Administering the VDN call profile . . . 62
Administering Avaya Visual Vectors . . . 63

High Availability backup and restore strategy

High availability backup strategy 65
Synchronizing after an unscheduled outage of the primary CMS server 65
Synchronizing after an unscheduled outage of the secondary CMS server 66

Appendix A: Backup and restore procedures

Avaya CMS backup strategy 67
Labeling the backup volume 67
Backup information format 68
How to interpret backup information 68

Appendix B: Items excluded from a CMSADM backup

Appendix C: Items backed up during a full maintenance backup

Appendix D: Restore characteristics of different data types

Appendix E: What to do if an Avaya CMS server fails

Appendix F: Frequently asked questions

Appendix G: Avaya CMS base load upgrade procedure for High Availability systems

Index 83

Preface

Overview

This document is written for customers who purchase the High Availability feature of the Avaya Call Management System (CMS).

Scope

This document describes procedures used to maintain your CMS High Availability (HA) system.

Contents

This document includes the following topics:

- Preface on page 7
- Introduction on page 17
- Primary and secondary CMS servers on page 25
- User scenarios on page 37
- High Availability backup and restore strategy on page 65
- Appendix A: Backup and restore procedures on page 67
- Appendix B: Items excluded from a CMSADM backup on page 69
- Appendix C: Items backed up during a full maintenance backup on page 71
- Appendix D: Restore characteristics of different data types on page 75
- Appendix E: What to do if an Avaya CMS server fails on page 77
- Appendix F: Frequently asked questions on page 79
- Appendix G: Avaya CMS base load upgrade procedure for High Availability systems on page 81

Reasons for re-issue

This is the first issue of this document.

Conventions

The following conventions are used in this document:

- Unless otherwise specified, all information and procedures in this document apply to the Sun Enterprise 3000, Sun Enterprise 3500, Sun Blade 100, and Ultra5 systems.
- Commands you enter from the console are shown in `courier` font.
- *Italic* text represents variable information.
- Many procedures in this document instruct you to “Enter” a command or some data. What is meant is that you must type the command or data as shown, and then press **Enter** or **Return** on your keyboard.
- Unless specified otherwise, the term CMS always implies Avaya Call Management System.

Related documents

Related documents lists sources for information related to contact center products and features. Not all documents are supported for all CMS releases or equipment.

To order Avaya documentation, call the Avaya Publications Center at 1-800-457-1235 (United States and Canada) or +1-410-568-3680 (outside the United States and Canada).

CMS software documents

Document title	Document number
Installing software on a CMS computer	
Avaya CMS Release 3 Version 11 Software Installation, Maintenance, and Troubleshooting Guide	585-215-115
CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance, and Troubleshooting	585-215-956
CentreVu Call Management System Release 3 Version 8 Software Installation, Maintenance, and Troubleshooting	585-210-941
Setting up a disk-mirrored system	
Avaya CMS Release 3 Version 11 Software Installation, Maintenance, and Troubleshooting Guide	585-215-115
CentreVu Call Management System Release 3 Version 9 Software Installation, Maintenance, and Troubleshooting	585-215-956
CentreVu Call Management System Release 3 Version 8 Disk-Mirrored Systems	585-210-940

Upgrade documents

There are several upgrade paths supported with CMS. For each of these upgrades, there is a document designed to support that upgrade. Note that none of the following upgrade documents are available from the publications center, but are available from the Avaya CMS documentation Web site.

- Base load upgrades

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

Document title
Avaya Call Management System Release 3 Version 11 Base Load Upgrades
CentreVu Call Management System Release 3 Version 9 Base Load Upgrade Procedures

- Platform upgrades and data migration

  A platform upgrade is used when upgrading to a new hardware platform (for example, upgrading from a SPARCserver 5 to an Enterprise 3500). 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 R3V11 or the latest load of the same CMS version). For R3V11, a specific set of instructions are written for the upgrade and are shipped to the customer site with the new hardware.

Document title
Avaya Call Management System Release 3 Version 11 Platform Upgrade and Data Migration
CentreVu Call Management System Release 3 Version 9 Platform Upgrade and Data Migration Instructions

- Avaya Call Management System Upgrade Express (CUE)

  CUE is used in the following conditions:

  — CMS is being upgraded from an earlier version (for example, R3V5u or R3V6) to the latest version (for example, R3V9 or R3V11).

  — The hardware platform is not changing.

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

Document title
Avaya Call Management System Release 3 Version 11 Sun Blade 100 Workstation CMS Upgrade Express
Avaya Call Management System Release 3 Version 11 Sun Blade 100 Workstation Mirrored System CMS Upgrade Express
Avaya Call Management System Release 3 Version 11 Sun Ultra 5 Computer CMS Upgrade Express
Avaya Call Management System Release 3 Version 11 Sun Enterprise 3000 Computer CMS Upgrade Express
Avaya Call Management System Release 3 Version 11 Sun Enterprise 3000 Computer Mirrored System CMS Upgrade Express
Avaya Call Management System Release 3 Version 11 Sun Enterprise 3500 Computer CMS Upgrade Express
Avaya Call Management System Release 3 Version 11 Sun Enterprise 3500 Computer Mirrored System CMS Upgrade Express
CentreVu Call Management System Release 3 Version 9 Sun Ultra 5 Computer CVUE Instructions
CentreVu Call Management System Release 3 Version 9 Sun Enterprise 3000 Computer CVUE Instructions
CentreVu Call Management System Release 3 Version 9 Sun Enterprise 3000 Computer Mirrored System CVUE Instructions
CentreVu Call Management System Release 3 Version 9 Sun Enterprise 3500 Computer CVUE Instructions
CentreVu Call Management System Release 3 Version 9 Sun Enterprise 3500 Computer Mirrored System CVUE Instructions

Hardware documents

Document title	Document number
Call Management System Sun Blade 100 Computer Hardware Installation, Maintenance, and Troubleshooting	585-310-783
Call Management System Sun Blade 100 Computer Connectivity Diagram	585-310-782
Call Management System Sun Enterprise 3500 Computer Hardware Installation, Maintenance, and Troubleshooting	585-215-873
Call Management System Sun Enterprise 3500 Computer Connectivity Diagram	585-215-877
Call Management System Sun Ultra 5 Computer Hardware Installation, Maintenance, and Troubleshooting	585-215-871
Call Management System Sun Ultra 5 Computer Connectivity Diagram	585-215-872
Call Management System Sun Enterprise 3000 and SPARCserver Computers Hardware Maintenance and Troubleshooting	585-214-016
Avaya Call Management System Terminals, Printers, and Modems	585-215-874

Switch documents

Document title	Document number
CMS Switch Connections, Administration, and Troubleshooting	585-215-876

Administration documents

Document title	Document number
Avaya Call Management System Release 3 Version 11 Administration	585-215-515
CentreVu Call Management System Release 3 Version 9 Administration	585-214-015
CentreVu Call Management System Release 3 Version 8 Administration	585-210-910

Other documents

Document title	Document number
Avaya CMS Open Database Connectivity	585-780-701
Avaya Call Management System Release 3 Version 11 LAN Backup User Guide	585-215-715
Avaya CMS R3V11 External Call History Interface	585-780-700
CentreVu CMS Release 3 Version 9 External Call History Interface	585-215-952
Avaya CMS Custom Reports	585-215-822
Avaya CMS Forecast	585-215-825
Avaya Visual Vectors Version 11 Installation and Getting Started	585-210-706
Avaya Visual Vectors Version 11 User Guide	585-210-709
Avaya Visual Vectors Version 9 Installation and Getting Started	585-210-947
Avaya Visual Vectors Version 9 User Guide	585-210-944

Documentation Web sites

For product documentation for all Avaya products and related documentation, go to http://www.avayadocs.com.

Important:
Additional information about new software or hardware updates will be contained in future issues of this book. New issues of this book will be placed on the web site when available.

Use the following web sites to view related support documentation:

- Information about Avaya products and service

  http://www.avaya.com.
- Sun hardware documentation

  http://docs.sun.com
- Okidata printer documentation

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

  http://www.informix.com
- Tivoli Storage Manager documentation

  http://tivoli.com/support/documents/public_manuals.html

If you have a problem

If you have a problem with a CMS High Availability configuration, call the Avaya Customer Care Helpline at 800-242-2121 to report the problem and obtain a case number. For customers outside the United States, please contact your local Avaya distributor or representative.

The Customer Care Helpline is staffed by trained Avaya CMS technicians at the Technical Service Center (TSC). The technicians at the TSC will try to fix your problem in a timely manner. If they cannot fix it, they will escalate the problem to a higher level of customer support.

When you call the Helpline, be sure to 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 Professional Services Organization (PSO) 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

Overview

The primary purpose of the Avaya CMS High Availability (HA) option is to ensure an uninterrupted data stream between the switch and the CMS system. With HA, two CMS servers are connected to one DEFINITY or MultiVantage™ system, thereby eliminating the traditional single point of failure between the CMS and the DEFINITY or MultiVantage system.

Both CMS servers collect data independently from the switch. 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 switch, or must be brought down for maintenance, the alternate server can carry the entire CMS activity load. Note that 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 HA option relies heavily on manual data synchronization between the two CMS servers, as well as on manual administration synchronization. Therefore, this document provides detailed descriptions of procedures needed to maintain synchronization between the two CMS servers.

The Avaya Professional Services Organization offers a package that will automate the synchronization between the two CMS servers. The auto-sync offer reduces the amount of time needed to maintain the HA servers. For more information, contact the Avaya Professional Services Organization at:

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

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 backup 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.

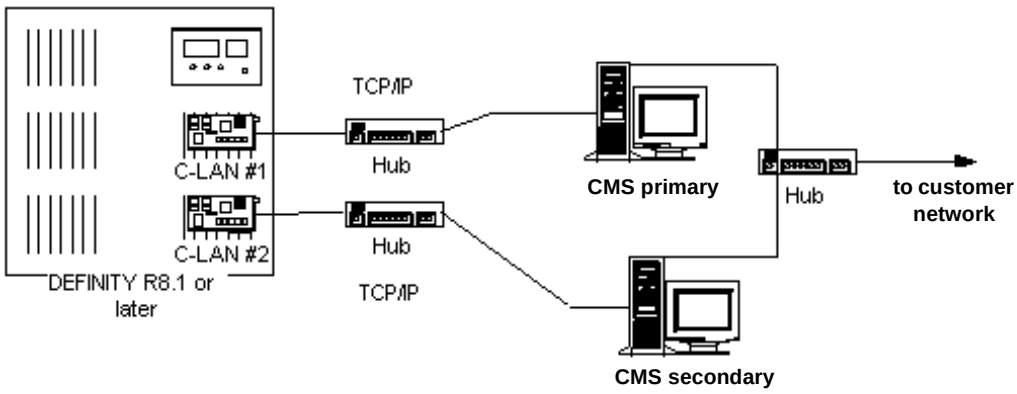
  At a minimum, manual switch-over entails the individual editing of CMS supervisor clients by their individual users in order to redirect them from the primary to the secondary server. Also, if the primary server is connected to one or more NTS servers, significant effort may be required to manually switch 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 77.

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. The C-LAN card provides TCP/IP connectivity between the switch and the CMS server. Each ACD link requires a separate C-LAN card and 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 switch back to both CMS servers. However, we strongly recommend performing administrative functions from only the primary CMS server.

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



Hardware platforms

CMS HA is supported on the following platform combinations:

- Sun Ultra 5 - Sun Ultra 5
- Sun Enterprise 3000 - Sun Enterprise 3000
- Sun Enterprise 3500 - Sun Enterprise 3000
- Sun Enterprise 3500 - Sun Enterprise 3500
- Sun Blade 100 - Sun Ultra 5
- Sun Blade 100 - Sun Blade 100

Note:

Use the following recommendations for HA configurations with different Sun platforms:

- For HA configurations in which Enterprise 3000 and 3500 servers are combined, the 3500 server should be designated as the primary HA server.
- For HA configurations in which Ultra 5 and Ultra 5 Einstein servers are combined, the Einstein server should be designated as the primary server.
- For HA configurations in which Sun Blade 100 and Ultra 5 servers are combined, the Sun Blade 100 server should be designated as the primary server.

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* is 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 69.

- **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 cards within the switch 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 uninterruptable 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 admin 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 switch 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 switch, and pump-up the ACD link.

  For more information, see Upgrading the CMS base load on page 38.

Primary and secondary CMS servers

Overview

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. It is highly recommended that you perform administration only on the primary CMS server, and administer from the secondary CMS server only when the primary is down. 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:

Primary CMS server	Secondary CMS server
May have Internet Call Center installed	Does not have Internet Call Center installed
Timetables turned on	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 Running timetables only on the primary server on page 54.

Both CMS servers collect data from the switch, 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 switch, or need to be shut down for maintenance, the alternate server can carry the entire CMS activity load.

Note:

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 admin 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.

CMS HA server maintenance

To assure that both CMS servers are functioning correctly and able to accept and process data from the switch, it is strongly recommended that the administrator, on a daily basis, perform the following functions on 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.
   a. Select **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.

WARNING:
Failure to adhere to the maintenance practices listed above may result in unnecessary loss of CMS data and/or incur additional administrative charges from Avaya technical support.

CMS recovery kit

Purpose

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.

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 CDs 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.

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

- Solaris 8 Software; CD-ROM disks 1 and 2
  - — also contains Solstice DiskSuite™
- Software Supplement for the Solaris 8 Operating Environment, contains:
  - — Sun Online Validation Test Suite (VTS)
- CMS Hardware Drivers CD-ROM, contains:
  - — High-Speed Serial Interface/Sbus (HSI/S) (required only for systems that have an HSI/S card)
  - — High-Speed Serial Interface/PCI (HSI/P) (required only for systems that have an HSI/P card)
  - — Serial Asynchronous Interface/PCI (SAI/P) drivers (required only for systems that have an SAI/P card)
- Annex Communication Server R10.0(B) Annex Host Tools CD-ROM (required only for systems using Network Terminal Server™ [NTS])
- Solstice™ for Server Connect, Version 9.2 CD-ROM (required only on systems using an X.25 link to a switch)
- INFORMIX® SQL Version 7.20 CD-ROM (optional)
- INFORMIX Dynamic Server (IDS) Version 9.21 CD-ROM
- INFORMIX SDK CD-ROM, contains:
  - — Runtime Enhanced SQL (ESQL)
- INFORMIX ILS CD-ROM
- Avaya Visual Vectors Server Software CD-ROM
- Avaya CMS Supplemental Services R3V11 CD-ROM
- R3V11 Avaya Call Management System (CMS) CD-ROM, also contains:
  - — Sun Solaris patches
  - — CMS patches
- Avaya CMS OPENLINK Open Database Connectivity (ODBC) Driver CD-ROM (optional)
- Avaya Visual Vectors Server Software CD-ROM

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 77.

Admin operations auto-synchronized by the switch

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

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

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

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

- Multi-agent skill change
- Change Agent skills

Admin 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:

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

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.

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

Admin 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
  - 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 50.

User scenarios

Overview

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.

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 81.

Changing 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.

Changing 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 switch and subsequently displayed on either CMS server.

Creating custom reports

R3V11 CMS High Availability requires that custom reports must exist on each CMS server in order to be run on each CMS server.

1. Create custom report on the primary CMS 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

R3V11 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 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
  1. Recreate the same designer report on the secondary CMS server.

Changing 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 - Synchronizing dictionary changes by back up and restore of ACD-specific administration data on page 41

  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.

- Method 2 - Synchronizing dictionary changes by backup and restore of specific tables on page 42

  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 - Synchronizing dictionary changes by back up and restore of ACD-specific administration data*. This process will manually synchronize the two CMS servers using the specific table backup and restore process.

- Method 3 - Administering the same dictionary changes on both the primary and secondary CMS servers on page 43

  Administer the same dictionary changes on both the primary and secondary CMS servers

Method 1 - Synchronizing dictionary changes by back up and restore of ACD-specific administration data

To synchronize dictionary changes by back up and restore of ACD-specific administration data:

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 admin 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:

      `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 - Synchronizing dictionary changes by backup and restore of specific tables

To synchronize dictionary changes by backup and restore of specific tables:

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:

      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.

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:

      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 3 - Administering the same dictionary changes on both the primary and secondary CMS servers

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 switch, 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 on and off External Call History

R3V11 CMS High Availability helps reduce the potential loss of External Call History (ECH) data sent to the ECH server because if the primary CMS server becomes inactive (e.g., CMS is down), you can start ECH on the secondary CMS and continue to collect data.

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

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

If your ECH 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 ECH. 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 46 - Changes the forecast data storage allocation on both servers individually.
- Method 2 on page 46 - Copies the forecast data storage allocation from the primary server to the secondary server.

Method 1

To change the forecast data storage allocation on both servers individually:

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

Instead of changing the forecast data storage allocation on both servers individually, you can do the following:

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, do the following:

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.

Administrating 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

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, do the following:

1. Administer the shortcut on the primary CMS server.
2. Back up the CMS Admin data on the primary CMS server.
3. Put the secondary CMS server in single-user mode.
4. Restore the CMS Admin 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, do the following:

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.

Refer to the Diagram of synchronizing CMS servers after data collection is turned on/off on page 53 for a depiction of the steps described in the procedure.

Synchronizing the CMS servers after turning data collection on/off	✓
At Time A, (see the Diagram of synchronizing CMS servers after data collection is turned on/off on page 53) 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.)	
Turn off data collection on the primary CMS server for all ACDs. Record the stop date and time.	Date/Time _____
Perform the desired administrative function (For example, Changing Data Storage Allocation).	
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.	Date/Time _____
Return the primary CMS server to multi-user mode.	
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 53) has run.	

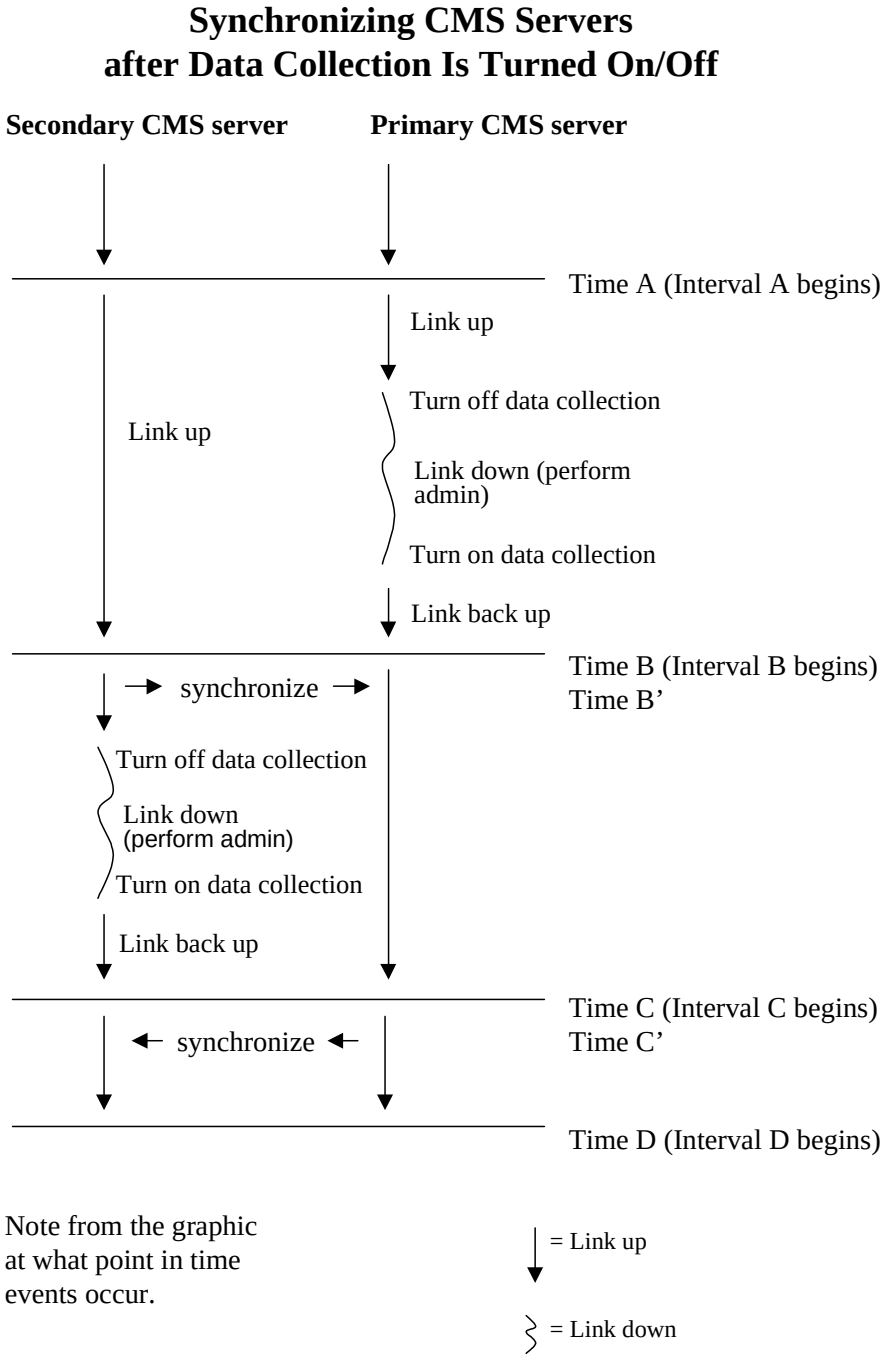
Synchronizing the CMS servers after turning data collection on/off	✓
At Time B‘ (see the Diagram of synchronizing CMS servers after data collection is turned on/off on page 53), perform an incremental historical backup of all ACDs on the secondary CMS server.	
Restore the historical data of specific start/stop and 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).	
Put the secondary CMS server in single-user mode.	
Turn data collection off on the secondary CMS server. Record the date and time.	Date/Time _____
Perform the same administrative function you did above for the primary CMS server on the secondary CMS server.	
Turn data collection “on” on the secondary CMS server. Record the date and time when the links come back up.	Date/Time _____
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 53), 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 53), 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.	Date/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.

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.

Diagram of synchronizing CMS servers after data collection is turned on/off



Running timetables only on the primary server

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

To do so, perform the following procedures:

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
```

   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.

   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, do the following:

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 to 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

Note:

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:

- Add the new user on the primary CMS server
- Then restore this new data to the secondary CMS server

1. Add users and user permissions on the primary CMS server.

   For more information, see “Administering user permissions” in *Avaya Call Management System Release 3 Version 11 Administration*, 585-215-515.

2. Perform a maintenance backup of CMS system administration data and ACD-specific administration data on the primary CMS server.

   For more information, see “Performing a Maintenance backup” in *Avaya Call Management System Release 3 Version 11 Administration*, 585-215-515.

3. Log in to the secondary CMS server and change to single-user mode.
4. 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 “Restoring data” in *Avaya Call Management System Release 3 Version 11 Administration*, 585-215-515.

5. Change the secondary server back to multi-user mode.
6. 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 Users - setting user passwords on page 61.

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.

Users - setting user passwords

Use this procedure 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:

   `su - cms`

5. Log in as root and enter:

   `passwd` ***`userid`***

   where ***`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:

   `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 if 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, do the following:

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

It is advisable to administer Avaya Visual Vectors from the primary CMS server only. By doing so, you will always know the most recent Visual Vectors information resides on the primary CMS server. Otherwise, you risk 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 switch 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.

High Availability backup and restore strategy

High availability backup 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: Backup and restore procedures on page 67.

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.

Synchronizing after an unscheduled outage of the primary CMS server

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

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

If you encounter an unscheduled outage of the secondary CMS server, perform the following procedure to re-synchronize it with the data in the primary CMS 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 *Avaya Call Management System Release 3 Version 11 Administration*, 585-215-515.
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.

Appendix A: Backup and restore procedures

The tape backup and restore procedures described in this Appendix 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.

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

0002llllll

00031234567

How to interpret backup information

Use this table to decode backup information.

Part #	Code	Meaning
1	CMS	System name
2	NNNNNN	Year, month and day of the backup, in the form yymmdd
3	NN	Number of backups for this day
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)

Appendix B: Items excluded from a CMSADM backup

A CMSADM backup copies all system directories and files, with the exception of the following:

- any swap devices (such as those displayed with “swap -l”)
- /proc
- /cdrom
- /n
- /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
- /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
- /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
- ttsctasks
- 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_dsplit (forecasting)
- f_dtkgrp (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

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 (e.g., 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.

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

If the links to both CMS servers are down:

1. 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 switch and the CMS system by connecting two CMS servers at one site to one MultiVantage™ system, thereby eliminating the traditional single point of failure between the CMS and the MultiVantage system.

Are the primary and secondary CMS servers aware of each other?

No. Both CMS servers collect data from the switch, 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.

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.

The following figure presents a conceptual illustration of a typical base load upgrade sequence for an HA system.

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.

Index

A

ACD
- administration data . . . 72
- Call Processing software . . . 19
- dual link . . . 79
- link failures . . . 22

administering
- Visual Vectors . . . 63

Agent Groups . . . 43
Agent Skills, changing . . . 39
Agent Trace, modifying . . . 37
Automatic Scripts . . . 48

B

Backup . . . 65
- CMSADM . . . 21
- files excluded from a CMSADM backup . . . 69
- labels . . . 67

C

Call Work Codes, updating . . . 38
C-LAN . . . 19
CMS
- required software . . . 29
- software failures . . . 22

CMS Server
- backup . . . 67
- changing timetables . . . 58
- data collected . . . 79
- failure . . . 77
- hardware failures . . . 22
- maintenance . . . 22, 27
- manual synchronization . . . 21
- operations on both . . . 32
- primary . . . 25
- running timetables . . . 56
- secondary . . . 25
- synchronizing . . . 50
- unscheduled outage . . . 65, 66
- upgrades . . . 23

CMS System Administration Data . . . 71
CMS Users
- new . . . 60
- removing . . . 61
- setting user passwords . . . 61

CMSADM Backup . . . 21
Custom Reports . . . 39
Customer Care Helpline . . . 15

D

Data Availability . . . 22
Data Collection
- synchronizing CMS servers . . . 50
- turned off . . . 36
- turned on . . . 46

Data Storage Allocation . . . 46
Designer Reports . . . 40
Dictionary . . . 41, 42
Dual ACD Links . . . 19, 79

E

Enhancements . . . 21

F

Forecast Data Storage Allocation . . . 46
Frequently Asked Questions . . . 79

H

Hardware
- failures . . . 22
- platforms . . . 20

Helpline . . . 15
High Availability, defined . . . 17, 79
Historical Data . . . 73

I

IL Number . . . 15
Incremental backup . . . 67
INFORMIX . . . 71
Interactive Scripts . . . 48
Internet Call Center . . . 25

M

Main Menu . . . 47
Maintenance Restores, non-disruptive . . . 21
Manually synchronizing servers . . . 21

O

Operations
- both CMS servers . . . 32
- data collection off . . . 36

P

Platforms, supported . . . 20
Prerequisites . . . 7
Primary CMS Server . . . 25
- failure . . . 77
- unscheduled outage . . . 65

publications center . . . 9

R

R3 migration, non-disruptive . . . 21
R3V8 Enhancements . . . 21
Recovery Kit . . . 28
Reports
- custom . . . 39
- designer . . . 40

Restore . . . 65

S

Secondary CMS Server . . . 25
- failure . . . 77
- unscheduled outage . . . 66

Shortcuts . . . 49
Software
- failures . . . 22
- Internet Call Center . . . 25
- shipped with CMS . . . 29

Split/Skill Call Profile . . . 49
Sun Enterprise 3000 . . . 8
Sun Enterprise 3500 . . . 8
Supported platforms . . . 20
Synchronization
- backup tapes . . . 65
- data . . . 26
- Main Menu additions . . . 47

T

TCP/IP . . . 19
Technical Service Center . . . 15
Timetables . . . 25
- changing server information . . . 58
- running on servers . . . 56

Troubleshooting . . . 77
TSC . . . 15

U

Ultra5 . . . 8
unscheduled . . . 65
Updating
- Agent Skills . . . 39
- Call Work Codes . . . 38

Upgrades
- base load . . . 38

V

VDN Call Profile Administration . . . 62