Using Avaya Call Management System High Availability

Release 21.0
Issue 2
November 2025

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H

(HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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 is not working on your company's behalf). Be aware that there can 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 Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

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

This document is written for:

- Avaya support personnel
- Contact center administrators

Users of this document must be familiar with CMS and the RHEL (Linux®) operating system.

Change history

The following table outlines changes in this document for Release 21.x:

Issue	Date	Summary of changes
1	June 2024	Minor corrections to general information only. There are no other content changes in this document for this release. For new HA configuration information, see *Avaya Call Management System High Availability Connectivity, Upgrade and Administration*.

Chapter 2: Introduction to High Availability

The primary purpose of the CMS High Availability (HA) option is to ensure an uninterrupted data stream between the Avaya Aura® Communication Manager system and the CMS server. With HA, two CMS servers are connected to one Communication Manager system, thereby eliminating the traditional single point of failure between the CMS and the Communication Manager system.

Refer to the product documentation for your CMS load for more information about supported Communication Manager system releases.

Both CMS servers collect data independently from the Communication Manager system. With few exceptions, both CMS servers provide full CMS capabilities. If either server fails, loses connection to the Communication Manager system, or must be brought down for maintenance, the alternate server can carry the entire CMS activity load. You must administer both CMS servers with an identical CMS setup including number of ACDs in the configuration, data storage allocation, users, and features.

The Avaya Professional Services (APS) organization offers a package that automates the synchronization between the two CMS servers. The Admin-Sync offer reduces the amount of time needed to maintain the HA servers and is required for most installations. For more information, contact APS at:

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

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

HA server switch-over after a failure event

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

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

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

- No switch-over

  If you do not require continuous access to your CMS data, you can elect not to switch-over to the secondary server after the primary server experiences a major failure event. When the primary server goes down, uninterrupted collection of call data will continue on the secondary server, but you may not be able to access that data until the primary server is restored.

- Manual server switch-over

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

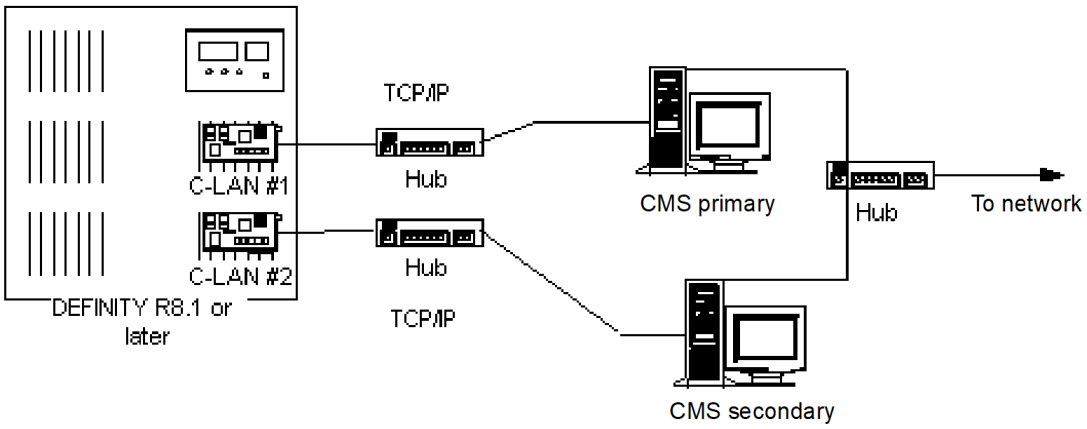
  At a minimum, manual switch-over entails the individual editing of CMS supervisor clients by their individual users in order to redirect them from the primary to the secondary server. Also, if the primary server is connected to one or more NTS servers, significant effort may be required to manually switch the NTS devices over to the secondary server. For more information about manual server switch-overs, see What to do if CMS server fails on page 56.

Dual ACD links

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

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

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



Increased data availability

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

- ACD link failures

  In the recommended HA configuration, ACD data is transmitted across different C-LAN circuit packs or ethernet ports within the Communication Manager system 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 HA option provides a duplicate CMS server. If a hardware failure occurs on one CMS server, data collection continues on the second CMS server. You can use the maintenance backup and restore process to recover the missing data onto the server that failed. If the CMS server fails, you may need to restore the CMSADM backup. Since you can do a CMSADM backup with data collection on, you can expect a good CMSADM backup and the system can be recovered more quickly.

- Power failures

  The primary and secondary servers should be separately connected to individual uninterruptible power supplies (UPS) on separate protected power circuits. This configuration

ensures that both servers will not be simultaneously disabled due to a localized power failure. However, in the event of an extended power outage, impacted servers should be shut down in order to prevent UPS failure and consequent possible data corruption on the server.

- CMS software failures

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

- CMS maintenance

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

- CMS full version upgrades

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

  For more information, see CMS base load upgrade on page 18.

Chapter 3: Primary and secondary CMS servers

When the CMS High Availability offer is installed, one CMS server is designated as the primary server, and the other is designated as the secondary server. It is highly recommended that you do administration only on the primary CMS server, and administer the secondary CMS server only when the primary is not functioning. To avoid possible confusion, label the servers as primary or secondary.

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

Primary CMS server	Secondary CMS server
Might have Internet Call Center installed	Does not ever 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 29.

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

The following operational practices are strongly recommended:

- Always do administration functions on the primary CMS server. Doing administration on both servers could lead to synchronization problems and loss of historical and/or administration data.
- Ensure that no users is 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 7.

The benefit to creating and following a routine where you always do administration on the primary CMS server and transfer (synchronize) the data to the secondary CMS server is that you can synchronize your data correctly.

Maintaining CMS HA server

About this task

In order to assure that both CMS servers are able to accept and process data correctly from the Communication Manager system, the administrator must do the following functions on a daily basis for both CMS servers.

The maintenance procedures listed below are not unique to the CMS HA offer. Therefore, you are probably already accustomed to doing these maintenance procedures on your previous CMS installation.

Caution:

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

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

Procedure

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

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

   ```
   Backups completed today: 1

   Status: Last backup finished at 10/02/00 00:23:41
   ```
4. Check the customer error log on both CMS servers for unusual errors.

CMS recovery kit

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

Recovery kit contents

Your CMS recovery kit must include the following:

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

Recovery kit software components

A number of software media are shipped with CMS. You must store this software with the recovery kit. Refer to the product software installation guide for your specific CMS release for more information about the specific software and software versions required for system recovery.

CMS requires the following software media:

- Operating System DVD
- Avaya Call Management System DVD (for specific OS)

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 What to do if CMS server fails on page 56.

Administration operations automatically synchronized by the Communication Manager system

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

Call center administration changes that are automatically synchronized via the Communication Manager system include:

- Changes to VDN Skill Preferences

- VDN assignments
- Vector contents

Agent Administration changes that are automatically synchronized via the Communication Manager system include:

- Multi-agent skill change
- Change Agent skills

Administration operations requiring manual synchronization

You cannot synchronize the following operations between the two CMS servers using the backup and restore process. Instead, you must do these operations 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 CMS 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

Call center administration

- VDN Call Profile
- Call Work Codes
- Split/Skill Call Profile

Administration operations synchronized by backups and restores

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

- Custom reports - additions or modifications to existing reports
- 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 doing 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 doing any of these operations, see Synchronize CMS after data collection is turned on/off on page 26.

Chapter 4: User scenarios

The following user scenarios refer to the CMS servers as primary and secondary. Do 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 do normal CMS tasks in your High Availability configuration so that the CMS servers are synchronized.

Modifying agent trace

Before you begin

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:

Procedure

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.

CMS base load upgrade

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 more information, see *Avaya Call Management System Base Load Upgrade*.

Modifying call work codes

Before you begin

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:

Procedure

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

Modifying agent skills

Procedure

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

   Note:

   The skill changes are written to the Communication Manager system and subsequently displayed on either CMS server.

Creating custom reports

Before you begin

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

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

Procedure

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

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

Method 1:

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

Method 2:

1. On the primary CMS server, copy the designer report to a file on PC or diskette. To copy a designer report from the primary server, do 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 CMS Supervisor **Copy** function to add the designer report. To copy a designer report onto the secondary server, repeat steps 1a through 1c; when the **Copy a Report** screen is displayed, select the **From a PC file to the CMS Server** option.

Method 3:

Recreate the same designer report on the secondary CMS server.

Modifying the Dictionary

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

Note:

On the primary CMS server, you can add, view, modify, and delete content. On the secondary CMS server, you can only view changes. You cannot add, modify, or delete content.

Choose one of the following procedures:

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

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

1. Do the Dictionary operation(s) on the primary CMS server.
2. On the primary CMS server, do 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. Ensure you back up and restore CMS system administration data if you change these Dictionary components.
4. Put the secondary CMS server in single-user mode.
5. Do ACD specific data restore for that same ACD on the secondary CMS server.
6. Return the secondary CMS server back to multi-user mode.

Method 2: Synchronizing Dictionary changes by backup and restore of specific tables

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. This process will manually synchronize the two CMS servers using the specific table backup and restore process.

1. Update Dictionary synonyms on the primary CMS server.
2. Do 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. Do 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. Update agent groups on the primary CMS server.
5. Do specific table backup for the synonyms table (synonyms) and agent groups table (groups) on the primary CMS server.
6. Do specific table restore for the synonyms and agent groups table on the secondary CMS server.

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

About this task

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

Call-based and interval-based exceptions are counted at the Communication Manager system, 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, do the following steps:

Procedure

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**.

Turn External Call History on and off

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

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

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

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

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

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

Administering forecast data storage allocation

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

Choose one of the following procedures:

Method 1: Changes 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: Copies the forecast data storage allocation from the primary server to the secondary server

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.

Administer 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

Procedure

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.

Administer 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 CMS Supervisor PC and login where they were created. The CMS supervisor is able to access the interactive scripts on the primary or secondary server irrespective of whether the supervisor is logged in to the primary or secondary server.

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

About this task

To administer shortcuts in a CMS High Availability configuration, do the following steps:

Procedure

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

Setting up the split/skill call profile

About this task

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, do 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:

Procedure

1. Access the **Call Center Administration: Split/Skill Call Profile Setup** screen.
2. Do the split/skill changes you require on the primary CMS server.
3. Do the split/skill call profile changes you require on the secondary CMS server.

Synchronize CMS after data collection is turned on/off

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

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

When any of the administrative changes listed above are undertaken, each CMS server should be taken down at different interval times in order to ensure that data is always being collected on the other server. The following image provides a depiction of the steps described in the Worksheet for synchronizing the CMS servers after turning data collection on/off on page 28.

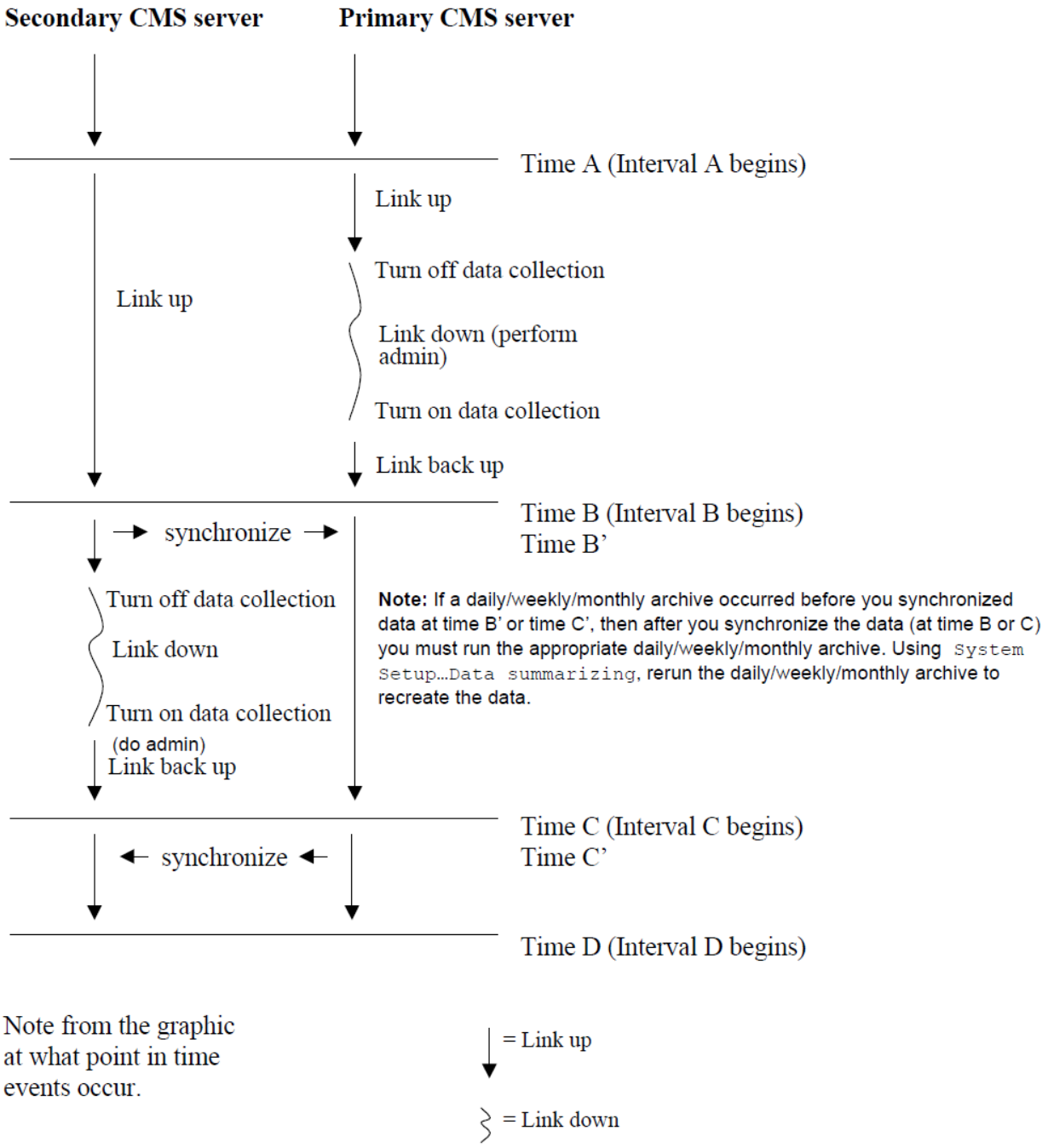


Figure 1: Synchronizing CMS Servers after Data Collection Is Turned On/Off

Worksheet for synchronizing the CMS servers after turning data collection on/off

Synchronizing the CMS servers after turning data collection on/off	Date/Time
At Time A, (see the) tell users to log off the primary CMS server. Put the primary CMS server in single-user mode. For more information, see *Administering Avaya Call Management System*.	
Turn off data collection on the primary CMS server for all ACDs. Record the stop date and time.	Date/Time _____
Do 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. For more information, see *Administering Avaya Call Management System*. 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 Figure 1: Synchronizing CMS Servers after Data Collection Is Turned On/Off on page 27) has run.	
At Time B (see the Figure 1: Synchronizing CMS Servers after Data Collection Is Turned On/Off on page 27), do 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 _____
Do 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 Figure 1: Synchronizing CMS Servers after Data Collection Is Turned On/Off on page 27), verify that the interval you are backing up has been archived on the secondary CMS server.	

Table continues…

Synchronizing the CMS servers after turning data collection on/off	Date/Time
At Time C' (see the Figure 1: Synchronizing CMS Servers after Data Collection Is Turned On/Off on page 27), do 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 doing 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 doing the backup and restore process.

Running timetables only on the primary server

About this task

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

To run a timetable from only the primary CMS server:

Procedure

1. Create a timetable on the primary CMS server.
2. **Enter** the timetable screen on the primary CMS server.

   At the bottom of the timetable screen you will see the following:

   ```
   This timetable will run on this or another CMS server

   < > Run only on this CMS server

   <X> Run on this or another CMS server
   ```

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

   The select option will appear as:

   ```
   This timetable will run on this or another CMS server
   ```

```
<X> Run only on this CMS server

< > Run on this or another CMS server
```

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

   At the bottom of the timetable screen you will see the following:

   ```
   This timetable will not run on this CMS server

   < > Run only on this CMS server

   < > Run on this or another CMS server
   ```

9. Accept the default setting.

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

   Note:

   To run the timetable from the secondary CMS server, 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 runs on both the primary and secondary CMS servers.

Running timetables on both primary and secondary servers

About this task

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.

To run a timetable from both the primary and secondary CMS servers:

Procedure

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
   ```

Editing timetables globally to change server ownership

About this task

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

The following procedure assumes that:

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

Important:

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

Procedure

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. Do 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. Do a CMS system administration backup on the primary server and restore it onto the secondary server.

Adding or modifying users

Procedure

1. Add the new user on the primary CMS server.
2. Restore the data to the secondary CMS server
3. Add users and user permissions on the primary CMS server.

   For more information, see the section about administering user permissions in *Administering Avaya Call Management System*.
4. Do a maintenance backup of CMS system administration data and ACD-specific administration data on the primary CMS server.

   For more information, see the section about doing a maintenance backup in *Administering Avaya Call Management System*.
5. Log in to the secondary CMS server and change to single-user mode.
6. Do a maintenance restore of CMS system administration data and ACD-specific administration data on the secondary CMS server for all ACDs.

   For more information, see the section about restoring data in *Administering Avaya Call Management System*.
7. Change the secondary server back to multi-user mode.
8. Log off the secondary server.

   Note:

   Maintenance restore of CMS system administration data replaces the user data and generates an operating system 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 Configure user passwords on page 34.

Removing users

Procedure

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

Configure user passwords

User passwords can be administered using CMS Supervisor or using the operating system. Passwords must be administered separately on each server.

For more information, see *Administering Avaya Call Management System*.

Administering the VDN call profile

Before you begin

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 the system restore ACD-specific administration data from the primary server to the secondary server, data in the archive interval in which the restore is performed is lost on the secondary server. Therefore, if minimization of data loss is of critical importance, after VDN call profile changes are made on the primary server, do 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:

Procedure

1. Access the **Call Center Administration: VDN Call Profile Setup** screen.

2. On the primary CMS server, do the VDN call profile administration changes you require.
3. Do the VDN call profile changes you require on the secondary CMS server.

Chapter 5: High Availability backup and restore strategy

High Availability configurations use the same tape backup procedures as standard CMS configurations. For more information about normal CMS server backup, restore process and schedule, see Backup and restore procedures on page 45 and CMS backup strategy on page 45.

You must maintain a set of dedicated synchronization tapes capable of holding one backup of each CMS server. Whenever you make a change to a CMS server to back up and restore to the other CMS server, do a manual backup using the dedicated synchronization tapes.

Synchronizing after an unscheduled outage of the primary CMS server

Before you begin

Ensure that users are temporarily logged into the secondary CMS server because the primary CMS server was not operational.

Procedure

1. After the primary CMS server is back up and running, note the date and time and do 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 required data.
7. Instruct users to log off the secondary CMS server and back into the primary CMS server.

Synchronizing after an unscheduled outage of the secondary CMS server

Procedure

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 about single-user mode, see *Administering Avaya Call Management System*.
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 required data.

Chapter 6: Resources

CMS and CMS Supervisor documents

CMS documentation is available on the Avaya Support website. Many of the latest customer documents are also available on the Avaya Documentation Center.

Title	Description	Audience
Overview		
Avaya Call Management System Overview and Specification	Describes tested product characteristics and product capabilities including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Sales engineers, Administrators
Installation, upgrades, maintenance, and troubleshooting		
Deploying Avaya Call Management System	Describes how to plan, deploy, and configure CMS on new VMware-based installations.	Implementation engineers
Deploying Avaya Call Management System in an Infrastructure as a Service Environment	Describes how to plan, deploy, and configure CMS on new Amazon Web Services and Google Cloud Platform installations.	Implementation engineers
Port Matrix for Avaya Call Management System	Lists the ports and connections used by CMS.	System administrators, support personnel
Upgrading Avaya Call Management System	Describes the procedures required to upgrade to a new CMS release.	Implementation engineers, system administrators
Avaya Call Management System Base Load Upgrade	Describes the procedures to upgrade from one base load (for example, 19.1.0.0) to another base load (for example, 19.1.0.1). Not all releases support base load upgrades.	Implementation engineers, system administrators
Maintaining and Troubleshooting Avaya Call Management System	Describes how to configure, maintain, and troubleshoot CMS.	System administrators, support personnel

Table continues…

Title	Description	Audience
Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting	Describes how to connect and administer the Communication Managerr systems used by CMS.	System administrators, support personnel
Avaya Call Management System High Availability Connectivity, Upgrade and Administration	Describes how to connect to HA servers and upgrade to HA.	System administrators, implementation engineers, and other software specialists
User guides		
Using ODBC and JDBC with Avaya Call Management System	Describes how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with CMS.	Administrators
Administration		
Administering Avaya Call Management System	Provides instructions on administering a contact center using CMS Supervisor.	Administrators
Avaya Call Management System Call History Interface	Describes the format of the Call History data files and how to transfer these files to another computer.	Administrators
Avaya Call Management System Database Items and Calculations	Describes each database item and calculation that CMS tracks and how CMS calculates the values displayed on CMS reports and CMS Supervisor reports.	Administrators, support personnel
Avaya Call Management System Custom Reports	Describes how to design and create custom reports in CMS.	System administrators
Avaya Call Management System Security	Describes how to implement security features in CMS.	System administrators, support personnel
CMS Supervisor		
Avaya CMS Supervisor Clients Installation and Getting Started	Describes how to install and configure CMS Supervisor.	Implementation engineers, administrators
Avaya CMS Supervisor Reports	Describes how to use CMS Supervisor reports.	Supervisors, administrators
Avaya CMS Supervisor Report Designer	Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard.	Supervisors, administrators

Avaya Solutions Platform Documents

Title	Description	Audience
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform server.	IT Management, sales and deployment engineers, solution architects, support personnel.
Installing the Avaya Solutions Platform 130 Series	Describes how to install Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel.
Maintaining and Troubleshooting Avaya Solutions Platform 130 Series	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel.
Avaya Solutions Platform 130 Series iDRAC9 Best Practices	Describes procedures to use the iDRAC9 tools on the Avaya Solutions Platform 130 Series servers.	Sales and deployment engineers, solution architects, support personnel.

AXP Private – Extended Scale

Title	Description	Audience
AXP Private – Extended Scale Solution Description	Describes tested product characteristics and product capabilities including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Sales engineers, Administrators
Administering AXP Private – Extended Scale	Provides instructions on administering AXP Private – Extended Scale.	Avaya support personnel, Administrators
Deploying AXP Private – Extended Scale	Describes how to plan, deploy, and configure AXP Private – Extended Scale.	Avaya support personnel
Maintaining AXP Private – Extended Scale	Perform maintenance and troubleshooting procedures for routine maintenance and troubleshooting ofAXP Private – Extended Scale.	Avaya support personnel, Implementation engineers, Administrators
Administering Application Enablement Services for AXP Private – Extended Scale	Provides instructions on administering Application Enablement Services for AXP Private – Extended Scale.	Avaya support personnel, Administrators

Table continues…

Title	Description	Audience
Migrating to AXP Private – Extended Scale	Describes migration procedures to AXP Private – Extended Scale.	Avaya support personnel, Administrators

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.

  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Appendix A: CMS backups and restores

Backup and restore procedures

The tape backup and restore procedures are identical to those used for non-high availability configurations. Because you are working with two servers, ensure that you label your backup tapes as primary and secondary.

For the maintenance or CMSADM backup procedures, see the section about maintaining a CMS data backup in *Administering Avaya Call Management System* or *Maintaining and Troubleshooting Avaya Call Management System*.

For the LAN backup procedure, see *Using Avaya Call Management System LAN Backup*.

CMS backup strategy

Since new data is written each day, you must back up the data regularly. Use a backup strategy appropriate to your call center. Managing the tapes (storage, security, and labeling) is key to ensure 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 always. 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).

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

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

You must perform a full maintenance backup nightly using multiple backup tapes in a regular rotation scheme.

You must perform a CMSADM backup at least one time per month.

Related links

[Label the backup volume](#) on page 46
[How to interpret backup information](#) on page 46

Label the backup volume

After a backup, the computer automatically labels your backup volumes. 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. Ensure to refresh your supply of backup tapes at appropriate intervals. For more information, see the documentation that came with your backup tapes.

Note:

The machines need to have matching tape drives and the appropriate tapes for those drives.

You must have the appropriate number of tapes for the backup. When you run a manual backup, which is not a scheduled backup 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. You do not need estimates for incremental backups as they fit on one tape.

Related links

CMS backup strategy on page 45

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 Number	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

Table continues…

Part Number	Code	Meaning
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 first position, an “L” displays if local System Administration data was backed up. or an “X” displays if no local System Administration data was backed up. In the second position, an “S” displays if system data was backed up or an “X” displays if system data was not backed up. In the third position, an “H”, “M”, “A”, or “X” displays. In the fourth position, a “C” or “X” displays. Any combination of letters identifying the type of backup can 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)

Related links

CMS backup strategy on page 45

Appendix B: Items excluded from a CMSADM backup

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

- /var/tmp
- /dump/tmp
- /cms/install/bin/restore
- /etc/system-release
- /etc/mtab
- /etc/nologin
- /etc/.name_service_door
- /var/spool/cups/tmp
- /var/spool/cups/temp
- /var/spool/cups/requests
- /var/spool/mqueue
- /var/lock/
- /var/spool/uucp/dummyech/Z
- /dev|/usr/dbtemp
- /usr/lib/cms/Aname
- /usr/lib/cms/Pname
- /usr/lib/cms/Sname
- /cms/cmstables
- /cms/db/inf/cms.dbs
- /cms/db/journal/shortcut
- /cms/db/journal/timetable
- /cms/pbx/master

- /cms/pbx/sim_pbx
- /cms/pbx/acd
- /cms/tmp
- /cms/dc/chr/chr_log
- /BI/add_on/data/forwarder
- /tmp
- /storage
- /INFORMIXTMP
- /var/spool/postfix/pid

Appendix C: Items backed up during a full maintenance backup

Note that a path name with one or more slashes (“/”) indicates an operating system file or directory. A path name 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 data is specific to the particular 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

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 the previously deleted rows, and any new data rows that may have been included in the actual restore range.

Appendix E: What to do if CMS server fails

Primary CMS server

One or more links to the primary CMS server goes down.

1. Log into your secondary CMS server and verify status of the links on it.
2. If the links are up on the secondary CMS server, inform your users that they must 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.

Primary CMS server is exhibiting problems

For example, users are unable to log in, reports do not run, missing archive intervals.

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

Primary CMS server goes down

1. Verify that your secondary CMS server is up and the links are up.
2. Inform your users that they must 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:

- Verify that your primary CMS server is up and the links are up.
- Call the Helpline and inform them you are a High Availability configuration and tell them the secondary CMS server is down.

Both CMS servers

Call the helpline, inform them you are a High Availability configuration and tell them links to both CMS servers are down. High Availability is not a Disaster Recovery system. If data is lost on both the CMS servers, you have lost data for the intervals in question.

Appendix F: Frequently asked questions

- What is the purpose of the CMS High Availability offer?

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

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

  No. Both CMS servers collect data from the Communication Manager system, but they operate 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 must do a server switch-over from the primary to the secondary HA server?

  Server switch-overs are not recommended for system outages of 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.

Index