Lucent Technologies
Bell Labs Innovations

CentreVu® Call Management System

Release 3 Version 8
High Availability User Guide

585-210-931
Comcode 108502204
Issue 1
June 2000

Copyright© 2000 Lucent Technologies
All Rights Reserved
Printed in U.S.A.

Notice

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

Your Responsibility for Your System's Security

Toll fraud is the unauthorized use of your telecommunications system by an unauthorized party, for example, persons other than your company's employees, agents, subcontractors, or persons working on your company's behalf. Note that there may be a risk of toll fraud associated with your telecommunications system and, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

You and your system manager are responsible for the security of your system, such as programming and configuring your equipment to prevent unauthorized use. The system manager is also responsible for reading all installation, instruction, and system administration documents provided with this product in order to fully understand the features that can introduce risk of toll fraud and the steps that can be taken to reduce that risk. Lucent Technologies does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunication services or facilities accessed through or connected to it. Lucent Technologies will not be responsible for any charges that result from such unauthorized use.

Lucent Technologies 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.

Canadian Department of Communications (DOC) Interference Information

This digital apparatus does not exceed the Class A limits for radio noise emissions set out in the radio interference regulations of the Canadian Department of Communications.

Le Présent Appareil Nomérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A préscrites dans le reglement sur le brouillage radioélectrique édicté par le ministére des Communications du Canada.

Trademarks

CentreVu and *DEFINITY* are registered trademarks of Lucent Technologies.

Sun, Sun Microsystems, SunOS, the *Sun* logo, *Solaris, Solstice, Solstice DiskSuite*, *Enterprise,* and *Ultra* are trademarks or registered trademarks of Sun Microsystems, Inc.

Exatape is a trademark of Exabyte Corporation.

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: Lucent Technologies Publications Center
Voice: 1-800-457-1235
International Voice: +1-317-361-5353
Fax: 1-800-457-1764
International Fax: +1-317-361-5355

Write: Lucent Technologies Publications Center
P.O. Box 4100
Crawfordsville, IN 47933
U.S.A.

Order: CentreVu CMS R3V8 High Availability Connectivity, Upgrade and Administration
Document No. 585-210-931
Comcode 108502204
Issue 1, June 2000

For additional documents, refer to the section entitled "Related Documents" in the Preface.

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 Lucent Technologies Publications Center.

Lucent Technologies National Customer Care Center

Lucent Technologies provides a telephone number for you to use to report problems or to ask questions about your call center. The support telephone number is 1-800-242-2121.

Document Support Telephone Number

Lucent Technologies provides telephone numbers for you to use to report errors or to ask questions about the information in this document. The support telephone numbers are:
Voice: 1-888-584-6366 and
International Voice: +1-317-322-6848.

European Union Declaration of Conformity

Lucent Technologies Business Communications Systems declares that the 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

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

Heritage Statement

Lucent Technologies—formed as a result of AT&T's planned restructuring—designs, builds, and delivers a wide range of public and private networks, communication systems and software, consumer and business telephone systems, and microelectronics components. The world-renowned Bell Laboratories is the research and development arm for the company.

Comments

To comment on this document, return the comment card at the front of the document.

Acknowledgment

This document was developed by the Lucent Technologies Information Development Organization for Global Learning Solutions.

CentreVu® Call Management System
Release 3 Version 8
High Availability Connectivity, Upgrade and Administration

Table of Contents

Preface P-1
Overview P-1
Scope P-1
Organization P-1
Conventions P-2
Related Documents P-2
If you have a problem P-2
Provide information P-3

1: Introduction 1-1
Overview 1-1
HA Server Switch-over After a Failure Event 1-1
Dual ACD Links 1-3
Hardware Platforms 1-4
R3V8 Feature Enhancements 1-4
Increased Data Availability 1-5

2: Primary and Secondary CMS Servers 2-1
Primary versus Secondary CMS servers 2-1
CMS HA Server Maintenance 2-2
CMS Recovery Kit 2-3
Purpose 2-3
Recovery kit contents 2-3
Recovery kit software components 2-3
Connectivity Considerations for CMS Server Switch-Overs . . . 2-4
Admin operations that are auto-synchronized by the switch . . 2-5
Admin operations that require manual synchronization 2-5
Admin operations synchronized by backups and restores. . 2-7
Operations that require data collection to be turned off 2-8

3: User Scenarios 3-1
Agent Trace - Modification 3-1
Base Load Upgrades with High Availability 3-1
Call Work Codes 3-2
Change Agent Skills 3-2
Custom Reports 3-2
Designer Reports 3-3
Dictionary Changes 3-4
Exceptions 3-7
External Call History - Turning on and off 3-8
Forecast Data Storage Allocation Administration 3-9
Forecasting Report Data, Administration 3-9
Main Menu Additions 3-10
Printers 3-10
Scripting 3-10
Shortcuts 3-10
Split/Skill Call Profile Setup 3-11
Synchronizing the CMS servers after turning Data Collection On/Off 3-12
Timetables – Running only on the Primary server 3-16
Timetables – Running on both Primary and Secondary servers . 3-17
Timetables – Global edits to change server ownership 3-18
Users - Adding or modifying 3-20
Users - Removing 3-20
Users - Setting User Passwords. 3-21
VDN Call Profile Administration 3-21
Visual Vectors - Vector Changes 3-22

4: High Availability Backup & Restore Strategy 4-1
High Availability Backup Strategy 4-1
Synchronizing after an unscheduled outage of the Primary CMS server 4-1
Synchronizing after an unscheduled outage of the Secondary CMS server 4-2

A: Backup & Restore Procedures A-1
CMS Backup Strategy. A-1
Labeling the backup volume A-1
Backup information format A-2
How to interpret backup information A-2

B: Items excluded from a CMSADM backup B-1

C: Items backed up during a Full Maintenance backup C-1

D: Restore Characteristics of Different Data Types D-1

E: What to do if a CMS Server Fails. E-1

F: Frequently Asked Questions F-1

G: CMS Base Load Upgrade Procedure for High Availability Systems G-1

Index IN-1

Preface

Overview

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

Scope

This document contains a variety of procedures to help you maintain your CMS High Availability system. It assumes a minimum level of technical knowledge on the part of its readers to complete the procedures. It assumes, for example, that the reader knows how to perform backup and restore procedures for the CMS system. Where necessary, this document refers to other CMS documentation which describe how to perform basic CMS procedures.

Organization

This document includes the following topics:

- Introduction

  Provides an overview of the new dual ACD links feature and R3V8 CMS High Availability

- Primary and Secondary CMS Servers

  Describes the two CMS servers and how to synchronize the data between them

- User Scenarios

  Describes step by step procedures to complete the most common High Availability scenarios you will encounter

- High Availability Backup & Restore Strategy

  Explains the High Availability backup and restore strategy and lists step by step procedures to complete backup and restore procedures

  Backup & Restore Procedures

  Items excluded from a CMSADM backup

  Items backed up during a Full Maintenance backup

  Restore Characteristics of Different Data Types

  What to do if a CMS Server Fails

  Frequently Asked Questions

  CMS Base Load Upgrade Procedure for High Availability Systems

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, and Ultra5 computers. They will be referred to as the "CMS server."
- Commands you enter from the console are shown in `courier` font.

Related Documents

To order any of these documents, call the Publications Center at 1-800-457-1235, or 1-317-361-5353.

- *CentreVu* CMS R3V8 Upgrades and Migrations (585-210-913)
- *CentreVu* CMS R3V8 Software Installation & Setup (585-210-941)
- *CentreVu* CMS R3V8 Switch Connections and Administration (585-215-876)
- *CentreVu* CMS R3V8 Change Description (585-210-925)
- *CentreVu* CMS R3V8 External Call History Interface (585-210-912)

If you have a problem

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

The Customer Care Helpline is staffed by trained CentreVu® 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.

Provide information

When you call the Helpline, be sure to identify yourself as a CentreVu® CMS High Availability customer and be prepared to give the following information:

- Your full name, your organization, and a phone number where a Lucent Technologies representative can contact you about the problem
- The installation location (IL) number

  The IL number is a 10-digit number from a Lucent Technologies database that helps identify the details of your CentreVu® 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 CentreVu Supervisor)
- A description of the problem
- The type of service contract your organization has with Lucent Technologies, if any.
- Whether you have a Professional Services contract related to the High Availability option.

  If your system is not covered by warranty or a service contract, you will be invoiced for the Helpline troubleshooting. A service contract may provide coverage for business hours only or for 24-hours a day, 7 days a week. Alternatively, the contract may provide you with a technician dedicated to your installation. If you are uncertain about the details or expiration date of your service contract, contact you Lucent Technologies representative.

Chapter 1: Introduction

Overview

The primary purpose of the CMS High Availability offer is to ensure an uninterrupted data stream between the DEFINITY ECS and the CMS system, which is achieved by connecting two CMS servers at one site to one DEFINITY® system, thereby eliminating the traditional single point of failure between the CMS and the DEFINITY system.

Both CMS servers collect data from the DEFINITY®, but they operate completely independently and are not even aware of each other. With few exceptions (which will be discussed in detail later), both CMS servers provide full CMS capabilities. Should either server fail, lose connection to the DEFINITY®, or need to be brought down for maintenance, the alternate server can carry the entire CMS activity load. Note that both CMS servers have to be administered with identical CMS Setup (number of ACDs in the configuration, data storage allocation, users, features, etc.).

The High Availability offer relies heavily on manual data synchronization between the two CMS servers as well as manual administration synchronization. Therefore, this document will discuss in detail procedures you will follow 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 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.

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

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

1. **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.

2. **Customized software switch-over**

   If the HA primary and secondary servers connect to CMS clients and other peripherals, such as NTS servers, printers, etc. over the same network subnet, LAN traffic on this “user” network can be automatically redirected from the primary to the secondary server by means of customized scripting tools set up by the Lucent Professional Services Organization (PSO). The scripts create an alias for the IP address of the primary server on the secondary server.

3. **Manual server switch-overs**

   If your HA servers do not connect to your user network over the same subnet, the custom software switch-over solution offered by the PSO can not be implemented. If you still require uninterrupted access to CMS data, the server switch-over must be performed manually.

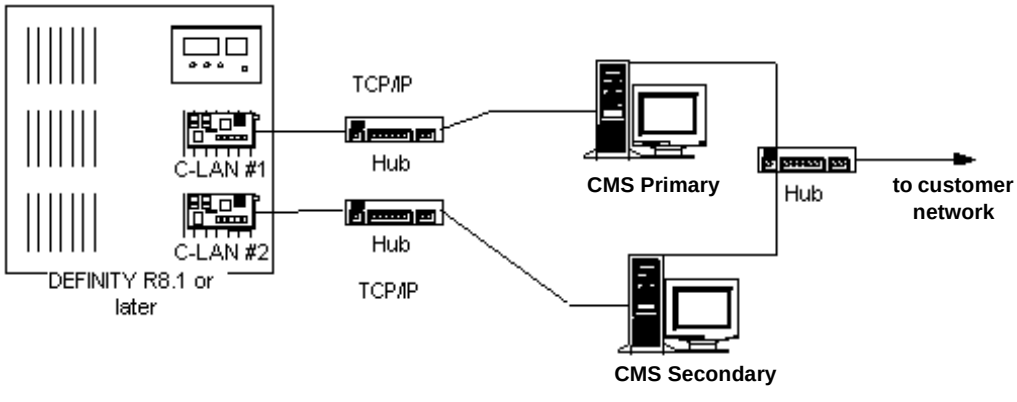
   At a minimum, manual switch-over entails the individual editing of host configuration files on the secondary server and re-administration of CMS supervisor clients by their individual users in order to redirect them from the primary to secondary server. Also, if the primary server is connected to one 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 a CMS Server Fails”**.

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 DEFINITY® 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 will send 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 will be able to perform call center and agent administration, and the results will be communicated from the DEFINITY® switch back to both CMS servers. However, as we discuss in detail later, 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 Definity ECS 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 - *Ultra* 5
- *Sun Enterprise*[†] 3000 - *Enterprise* 3000
- *Sun Enterprise* 3500 - *Enterprise* 3000
- *Sun Enterprise* 3500 - *Enterprise* 3500

Note:

- For HA systems in which *Enterprise* 3000 and 3500 servers are combined, the 3500 server should be designated as the primary HA server
- for HA systems in which Ultra 5 and Ultra 5 Einstein servers are combined, the Einstein server should be designated as the primary server

R3V8 Feature Enhancements

The following improvements have been made to the standard R3V8 CMS offer and apply to all standard R3V8 CMS platforms supported (i.e., not just High Availability platforms). These new features were designed to prevent data loss and improve system availability.

1. **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 that 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 "Items excluded from a CMSADM backup".
2. **Manually synchronize the two CMS systems**: The following capabilities were incorporated into CMS to allow you to manually synchronize two independent R3V8 CMS servers in a High Availability configuration:
    a. non-disruptive maintenance restores - non-disruptive maintenance restores is 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.

**Ultra* is a trademark of Sun Microsystems, Inc.
†*Enterprise* is a trademark of Sun Microsystems, Inc.

b. non-disruptive R3 migration - non-disruptive R3 migration is 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 (e.g., R3V6 to R3V8 or R3V8.1 to R3V8.2 when database schema changes are required).

3. **Capability to turn External Call History (ECH) on and off**: The ECH feature can be independently started and stopped on the two HA servers. How ECH is managed depends on your particular CMS configuration:
   - if you do not use any customized CMS reporting solutions (developed by the PSO), ECH data should be active only on the primary server under normal operating conditions. If the primary server fails, ECH can be started on the other CMS server.
   - if you do use customized CMS reporting solutions developed by the PSO, ECH data should be active on both CMS servers. Consult with your PSO representative for details.

Increased Data Availability

The R3V8 CMS High Availability offer builds on the availability and serviceability improvements implemented in the standard R3V8 CMS offer described above. Below is a summary of how the R3V8 CMS High Availability offer increases the availability of your CMS data.

1. **ACD link failures**: In the recommended HA configuration, ACD data is transmitted across different C-LAN cards within the DEFINITY® 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 R3V8 CMS server. You will use the maintenance backup and restore process to recover the missing data onto the R3V8 CMS server that was connected to the down ACD link.
2. **CMS hardware failures**: The R3V8 CMS server is duplicated. If a hardware failure occurs on one R3V8 CMS server, data collection continues on the second R3V8 CMS server. You will use the maintenance backup and restore process to recover the missing data onto the R3V8 CMS server that failed. If the R3V8 CMS system fails, you may need to restore the cmsadm backup. Since the cmsadm backup can now 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.

3. **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 powered down in order to prevent UPS failure and consequent possible data corruption on the server.
4. **CMS software failures**: The R3V8 CMS application is duplicated. If the CMS application fails or a CMS data collection process fails on one R3V8 CMS server, data collection continues on the second R3V8 CMS server. You will use the maintenance backup and restore process to recover the missing data onto the R3V8 CMS server with the software problems.
5. **CMS maintenance**: You will not lose data during either a cmsadm backup or a maintenance backup. You will not lose data when restoring a maintenance backup as long as you are **not** restoring Local System Admin data.
6. **CMS full version upgrades**: In a High Availability configuration, one CMS server continues to collect data while the other CMS server is being 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. Note that if you upgrade the DEFINITY® with a new release, the interval of data loss is limited to the amount of time it takes to administer the latest Call Center Release on the DEFINITY® and pump-up the ACD link. (See the “Base Load Upgrades with High Availability” section later in this document.)

Chapter 2: Primary and Secondary CMS Servers

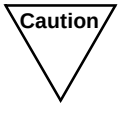
Primary versus Secondary CMS servers

When the CMS High Availability offer is installed at your location, you designate one CMS server to be the “Primary” and the other 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 to indicate which is the primary and secondary.

The Primary and Secondary servers are essentially identical, except for the following differences.

Primary CMS Server	Secondary CMS Server
May have Internet Call Center loaded	Does not have Internet Call Center loaded
May have External Call History turned on	Does not have External Call History turned on
Has timetables turned on	Timetables turned off, except for incremental and full backup timetables and any others you want to run on both CMS servers. (See the “Timetables – Running only on the Primary server” section in this guide for more details.)

Both CMS servers collect data from the DEFINITY®, but they operate completely independently and are not even aware of each other. Both CMS servers provide full CMS capabilities except for the differences listed above. Should either server fail, lose connection to the DEFINITY®, or need to be brought down for maintenance, the alternate server can carry the entire CMS activity load.



It is strongly recommended that you always perform administration functions on one CMS server (designated the “Primary” CMS server) and use the “Secondary” CMS server as a backup. Performing administration on both servers could lead to synchronization problems and loss of historical and/or admin data.

Caution

It is strongly recommended that no users are 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 specific switch-over strategy, as discussed in "HA Server Switch-over After a Failure Event" on page 1.

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 healthy and able to accept and process data from the DEFINITY ECS, 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. To do this, select `Maintenance > Archiving Status` from the CMS menu; press Enter to access the action list in the top right corner of the `Maintenance: Archiving Status` window, then press Enter again to view archive status information for all ACDs.
3. To verify that daily backups have run, select `Maintenance > Backup Data` from the CMS menu; at the top of the `Maintenance: Backup Data` window, output similar to the following example is displayed:

   ```
   Backups completed today: 1
   Status: Last backup finished at 05/02/00 00:23:41
   ```

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

Note that these maintenance procedures are not new or in any way unique to the CMS High Availability offer. You are probably already accustomed to performing these maintenance procedures on your existing CMS server.

WARNING:

Failure to adhere to the maintenance practices listed above may result in unnecessary loss of CMS data and/or incur additional administrative charges associated with Lucent Technical Support.

CMS Recovery Kit

Purpose

The recovery kit consists of the backup media and original software that the Lucent 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 contents:

- the latest **cmsadm** file system backup tapes
- latest full maintenance backup tapes
- patching CDs and tapes

Recovery kit software components

A number of software packages are shipped with your CentreVu® CMS. It is recommended that you store this software with the recovery kit.

The following table lists the required and optional software components used in CMS R3V8, along with the HA server platforms to which they apply (E3000, E3500, and *Ultra** 5).

Software Component	HA Server Platform	Required/ Optional
Sun Solaris 7 operating system (3/99 version)	All	Required
Sun Online Validation Test Suite (VTS) 3.1	All	Required
Bay Networks Annex R10.0B drivers	All	Optional
*INFORMIX** Structured Query Language (SQL) Version 7.20 *INFORMIX*† Standard Engine (SE) Version 7.22 *INFORMIX*‡ Runtime Enhanced SQL (ESQL) Version 9.14 *INFORMIX*§ International Language Supplement (ILS)	All All All All	Optional Required Required Required
Solstice DiskSuite 4.2 software (found on the "*Solaris* Easy Access Server" CD).	All	Required
CMS Supplemental Services software	All	Required
CMS application software	All	Required

* *Ultra* is a trademark of Sun Microsystems, Inc.

Software Component	HA Server Platform	Required/ Optional
Open Database Connectivity (ODBC) software	All	Optional
Visual Vectors server software	All	Optional

*_Informix_ is a registered trademark of Informix Software, Inc.
†_Informix_ is a registered trademark of Informix Software, Inc.
‡_Informix_ is a registered trademark of Informix Software, Inc.
§_Informix_ is a registered trademark of Informix Software, Inc.

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 time and effort required to accomplish an HA server switch-over depends on your particular network configuration:

- if the primary and secondary server are linked to your user network via a shared network subnet, the switch-over process can be accomplished by use of customized scripts developed by the Lucent Professional Services Organization (PSO). The custom scripts use the IP alias address for the primary server and temporarily assign it to the secondary server. This “software switchover” method enables switch-overs to be accomplished in a manner that is both fast and reliably error free. **Co-location of the HA primary and secondary servers on the same customer network is highly recommended so that the switch-over scripts can be set up for use in server switch-overs.**
- if the primary and secondary server are linked to your user network via different network subnets, the automated scripting method (described above) can not be used for HA server switch-overs. In this case, the switch from primary to secondary server must be done manually. The amount of effort required for a manual CMS server 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 a CMS Server Fails” .

Admin operations that are 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 Definity switch.

Call Center Administration changes which are auto-synchronized via the switch include:

- changes to VDN Skill Preferences
- VDN assignments
- vector contents

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

- Multi-agent Skill change
- Change Agent Skills

Admin operations that require 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

- Agent Exceptions
- Split/Skill Exceptions
- Trunk Group Exceptions
- VDN Exceptions
- Vector Exceptions

UNIX Administration

- Administering passwords

Scripting & Timetables

- Create Supervisor scripts (from a supervisor login)
- Scheduling of Time Tables

  Note on timetable scheduling:

  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, beaware 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

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

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
- CentreVu® Supervisor Designer Reports – additions or modifications to existing
- Dictionary operations
  - 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

- Shortcuts – additions or modifications to existing
- User Permissions
  - ACD Access
  - Feature Access
  - Main Menu Addition Access
  - Split/Skill Access
  - Trunk Group Access
  - User Data
  - Vector Access
  - VDN Access

Operations that require 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 still require data collection to be turned off while they are being performed. Therefore, 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 assistance in performing any of these operations, refer to the section of this User's Guide entitled "Synchronizing the CMS servers after turning Data Collection On/Off".

Chapter 3: User Scenarios

The following user scenarios refer to the 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 down. These user scenarios describe how to perform normal CMS tasks in your High Availability configuration so that the CMS servers are kept synchronized.

Agent Trace - Modification

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.

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.

Base Load Upgrades with High Availability

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 “CMS Base Load Upgrade Procedure for High Availability Systems”.

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. 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.

Change 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 DEFINITY® ECS and subsequently displayed on either CMS server.

Custom Reports

R3V8 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.

Designer Reports

R3V8 CMS High Availability requires that Designer reports must exist on each CMS server in order to be run on each CMS 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` buttom located near the bottoom 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 CentreVu 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.

Dictionary Changes

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.

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

Note that this procedure is for dictionary operations made on a single ACD. If you will perform dictionary operations on multiple ACDs, perform the backup for ***all*** ACDs and restore for ***all*** ACDs.

1. Perform the Dictionary operation(s) on the Primary CMS server.
2. On the Primary CMS server, perform ACD Specific Administration data backup for the ACD on which you made the changes.
3. Put the Secondary CMS server in single-user mode.
4. Perform ACD Specific Data restore for that same ACD on the Secondary CMS server.
5. Return the Secondary CMS server back to multi-user mode.
6. 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.

   Select option 2 from the turn on/stop menu to stop the Visual Vectors server software; to restart it, select option 1.

NOTE:

Be sure to specify `Current ACD` or `All ACDs` appropriately on the backup and restore, depending upon whether or not you changed dictionary items on multiple ACDs.

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.

Be sure to back up and restore CMS System Admin data if you change these dictionary components.

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

Dictionary synonyms and Dictionary agent groups can also be duplicated using the specific table backup and restore process shown below. The specific table backup and restore process *takes less time* than using the ACD Specific Administration data backup described above. Using the process described below, you will manually synchronize the two CMS servers using the specific table backup and restore process.

Dictionary Synonyms

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, move the cursor to the Select tables option and press Enter once again.
    d. Select the synonyms and then press Enter to access the Action List in the top right corner of the screen.
    e. 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, move the cursor to the Select tables option and press Enter once again.
    d. Select the synonyms and then press Enter to access the Action List in the top right corner of the screen.
    e. 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; to restart it, select option 1.

Agent Groups

1. Update Agent Groups on the Primary CMS server.
2. Perform specific table backup for the Synonyms table (synonyms) and Agent Groups table (agroups) on the Primary CMS server.
3. Perform specific table restore for the Synonyms and Agent Groups table on the Secondary CMS server.
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.

5. Select option 2 from the turn on/stop menu to stop the Visual Vectors server software; to restart it, select option 1.

Method 3: A third method is to simply 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.

Exceptions

Exceptions must be administered individually on each HA server.

Note:

There are three basic types of Exceptions: call-based, interval-based or 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 excetion 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.

External Call History - Turning on and off

R3V8 CMS High Availability helps reduce the potential loss of ECH data sent to the External Call History 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 any customized CMS reporting solutions developed by Lucent PSO, ECH data should be active on only one CMS server at a time. If that CMS server fails, then ECH can be turned off on the failed CMS server and activated on the other CMS server. Adding the capability to turn ECH on and off minimizes the amount of ECH data lost in the event of a CMS server failure.

If you do use customized CMS reporting solutions developed by Lucent PSO, ECH data should be active on both CMS servers. Consult with your PSO representative for details.

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.)

  If the link is not down on the Secondary CMS server, turn ECH “on” on the Secondary CMS server and indicate “Yes” when the system asks you whether you want to “Send the buffered data.” Then, turn ECH off on the Primary CMS server. See the *CentreVu CMS R3V8 External Call History Interface* document.

NOTE:

- If some ACDs are still collecting data on the Primary CMS server, turn ECH off on the Primary so that you do not collect duplicate data now that the Secondary is collecting ECH data.
- Some of the buffered data may be duplicate data.
- When the Primary CMS server comes back up, you must turn External Call History off on the Secondary CMS server and back “on” on the Primary CMS server.

Contact your Lucent 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. For help outside the U.S., contact your local Lucent distributor or representative.

Forecast Data Storage Allocation Administration

R3V8 CMS High Availability permits data collection to remain on during forecasting data storage allocation.

Method 1:

1. Change the Forecast Data Storage Allocation on the Primary CMS server.
2. Change the Forecast Data Storage Allocation on the Secondary CMS server.

Method 2:

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.

Forecasting Report Data, Administration

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.

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, the Main Menu Additions will appear on the Secondary CMS server but the associated files will not. Therefore, these files also need to be copied onto the secondary server.

Printers

Printers are not shared between the two CMS servers. Therefore, 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 CentreVu® Supervisor PC and login in which they were created. It does not matter whether the CentreVu® Supervisor is logged into the Primary CMS server or Secondary CMS server (if the Primary is down) – either way, the CentreVu® 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.

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.

Split/Skill Call Profile Setup

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.

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 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 also be lost on the Secondary server. Therefore, 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 the CMS servers after turning Data Collection 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 figure on page 14 for a depiction of the steps described in the procedure.

Synchronizing the CMS servers after turning Data Collection On/Off	✓
1. At Time A, tell users to log off the Primary CMS server.	
2. Put the Primary CMS server in single-user mode (see CentreVu® CMS Administration manual.)	
3. Turn off data collection on the Primary CMS server for all ACDs. **Note the stop date and time**.	**Date/Time** _____
4. Perform the desired Administrative function (e.g., Changing Data Storage Allocation).	
5. Turn data collection back “on” on the Primary CMS server, and verify that all the links come back up. (See CentreVu® CMS Administration manual.) **Note the date and time** when the links come back up.	**Date/Time** _____
6. Return the Primary CMS server to multi-user mode.	

Synchronizing the CMS servers after turning Data Collection On/Off	✓
7. 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 has run.	
8. At Time B‘ (see graphic), perform an incremental historical backup of all ACDs on the Secondary CMS server.	
9. 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 e.g., 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 (continuing with our example, if the link went down at 5:13 and came back up at 5:19, enter 5:29 as the stop time). **Note:** **The correct format used when defining start/stop dates to restore historical data is: mm/dd/yy**	
10. Put the Secondary CMS server in single-user mode.	
11. Turn data collection off on the Secondary CMS server. **Note the date and time.**	**Date/Time** _____
12. Perform the same administrative function you did above on the Primary CMS server on the Secondary CMS server.	
13. Turn data collection “on” on the Secondary CMS server. **Note the date and time** when the links come back up.	**Date/Time** _____
14. Put the Secondary CMS server in multi-user mode.	
15. After the ACD links come back up, wait for the end of that interval.	
16. At Time C (see graphic), verify that the interval you are backing up has been archived on the Secondary CMS server.	

Synchronizing the CMS servers after turning Data Collection On/Off	✓
17. At Time C' (see graphic), perform an incremental backup of all ACDs on the Primary CMS server. **Note:** If a Daily/Weekly/Monthly archive occurred before you synchronize 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.	
18. Restore the Historical data of specific start/stop and dates/times of all ACDs to the Secondary CMS server. Continuing with the example introduced in step 10 above, 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** _____

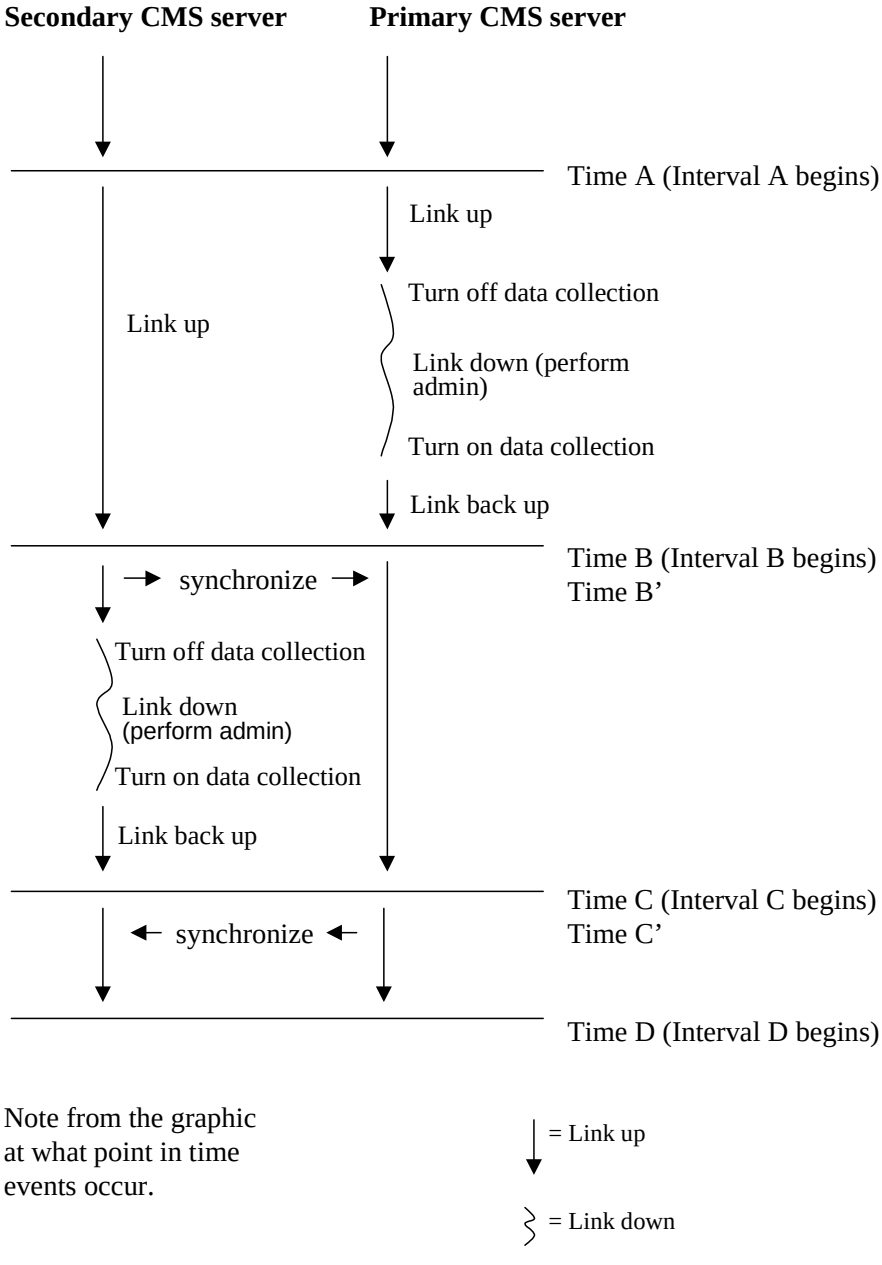
Note that in this scenario the link was down for only a single interval in both the Primary and Secondary CMS servers. Of course, the link might be down for multiple intervals. If the link is down for multiple intervals, wait until the link has come back up before performing the backup and restore process, no matter how many intervals it takes to come back up.

It is critical that you wait until the most recent interval during which the link came back up has been archived before performing the backup and restore process.

NOTE:

If a Daily/Weekly/Monthly archive occurred before you synchronize 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.

Synchronizing CMS Servers after Data Collection Is Turned On/Off



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

= Link up

= Link down

Timetables – Running 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.
9. 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.

Timetables – Running on both Primary and Secondary servers

There may be instances where 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. You will see the following:

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

   Accept the default selection.
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 using Maintenance Back Up Data.
6. On the secondary server, change CMS to single-user mode.
7. Restore the data on the Secondary CMS server using Maintenance Restore.
8. Change CMS back to multi-user mode on the secondary server.
9. 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
```

Timetables – Global edits 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:

Be aware that, if you make administation changes on the Secondary server during the interval in which the primary server is down, and you wish to transfer those changes to the Primary server after it is restored, this will require additional effort to restore timetables to the 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, if possible.

1. Log into the Secondary CMS server as "cms", so you have permission to globally edit all user's 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.

NOTE:

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:
   a. If you have not made any CMS administration changes on the Secondary server (including timetable modifications or revisions) which 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. **The remaining steps (presented below) can be disregarded.**
   b. If you have made any CMS administration changes on the Secondary server and you wish to transfer them to the Priamry 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.
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.

Users - Adding or modifying

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 user(s) via User Data on the Primary CMS server (for details see *Assigning User Data*, Chapter 9 in: CentreVu® CMS Administration, 585-210-910).
2. Add user(s) Permissions on the Primary CMS server (for details, see *Assigning User Data*, Chapter 9 in: CentreVu® CMS Administration, 585-210-910).
3. Do maintenance backup of CMS system administration data and ACD-specific administration data on the Primary CMS server (for details, see *Running a Maintenance Backup*, Chapter 11 in: CentreVu® CMS Administration, 585-210-910).
4. Log in to the Secondary CMS server and change to single-user mode.
5. Do maintenance restore of CMS system administration data and ACD-specific administration data on the Secondary CMS server for all ACDs (for details, see *Running a Restore*, Chapter 11 in: CentreVu® CMS Administration, 585-210-910).
6. Change the Secondary server back to multi-user mode.
7. 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 (see "Users - Setting User Passwords", below).

Users - Removing

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.

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 are done administering user passwords, enter:

   ```
   exit
   ```

9. The system returns to the CMS main menu.

VDN Call Profile Administration

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.

Note:

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 also 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 required.
3. Perform the VDN Call Profile changes you require on the Secondary CMS server.

Visual Vectors - Vector Changes

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

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 CentreVu® Visual Vector server data via the setupaas menu.
5. Log in to the Secondary CMS server and restore CentreVu® Visual Vector server data via the setupaas menu.

NOTE:

Vector changes (except vector comments) are written to the DEFINITY® and subsequently reflected on both CMS servers regardless of which server (Primary or Secondary) is in use.

Backing up and restoring Visual Vectoring server data must be performed after each session where vector changes are made or you risk losing Visual Vector comments.

Chapter 4: High Availability Backup & Restore Strategy

High Availability Backup Strategy

With your High Availability configuration you will essentially follow a traditional backup routine for two CMS servers instead of just one. Therefore, follow the normal CMS server backup/restore process and schedule for traditional, non-High Availability systems as described in "Backup & Restore Procedures".

In addition, have a set of dedicated ***synchronization*** tapes capable for one backup of ***each*** CMS server. 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.

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 down.

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. On the Primary CMS server, restore both the ACD-specific and CMS Administration data from the Secondary CMS server full maintenance backup (only if you made administration changes on the Secondary CMS server while the Primary was down).
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 procedures below to resynchronize 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. (See CentreVu® CMS Administration manual.)
3. On the Secondary CMS server, restore both the ACD-specific and CMS Administration data from the Primary CMS server full maintenance backup (only if you made administration changes on the Primary CMS server while the Secondary was down).
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.

   Note:

   The correct format for the dates specified for the historical data restore is: mm/dd/yy

Appendix A: Backup & Restore Procedures

Essentially the procedure to back up and restore the CMS servers in a High Availability configuration is the same as it was with just a single CMS server, except that now you are working with two independent servers instead of one. The backup and restore procedures described in this Appendix are identical to those used for non-High Availability configurations. Because you are working with two servers, be sure to label your backup tapes carefully, “Primary” and “Secondary.”

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 2 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 CentreVu® 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. CentreVu® 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 1 tape so no estimate is needed.)

Backup information format

```
0001    CMS-NNNNNN-NN-LLLL-NN-L-NN
0002     I      I  I  I  I  I  I
0003     1      2  3  4  5  6  7
```

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 All ACDs 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 CMS server on which it was administered. This data can only be restored onto the server from which it was copied.

CMS System Administration Data: This is administrative data that is not ACD-specific, such as:

- user data
- timetables
- custom reports

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

ACD-Specific Administration Data: This is data which is specific to a particular ACD. It includes:

- 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: This data includes interval, daily, weekly, and monthly archived call data. In addition, historical data also includes *event* data, which conists 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 which 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 which may have been included in the actual restore range.

Appendix E: What to do if a 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).
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. Contact your CMS technical support organization/representative and inform them that 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. Contact your CMS technical support organization/representative 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. Contact your CMS technical support organization/representative 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. Contact your CMS technical support organization/representative 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. Contact your CMS technical support organization/representative and inform them you are a High Availability configuration and tell them links to both CMS servers are down.

If there is an unscheduled outage of both servers:

1. Contact your CMS technical support representative. 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 CMS High Availability offer? The purpose of the CMS High Availability offer is to ensure data availability between the DEFINITY ECS and the CMS system by connecting two CMS servers at one site to one DEFINITY® system, thereby eliminating the traditional single point of failure between the CMS and the DEFINITY system.

What platforms support the CMS High Availability offer? UE3000-UE3500, UE3500-UE3500, UE3000-UE3000, and Ultra5-Ultra5.

Are the Primary and Secondary CMS servers aware of each other?

No. Both CMS servers collect data from the DEFINITY®, 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.

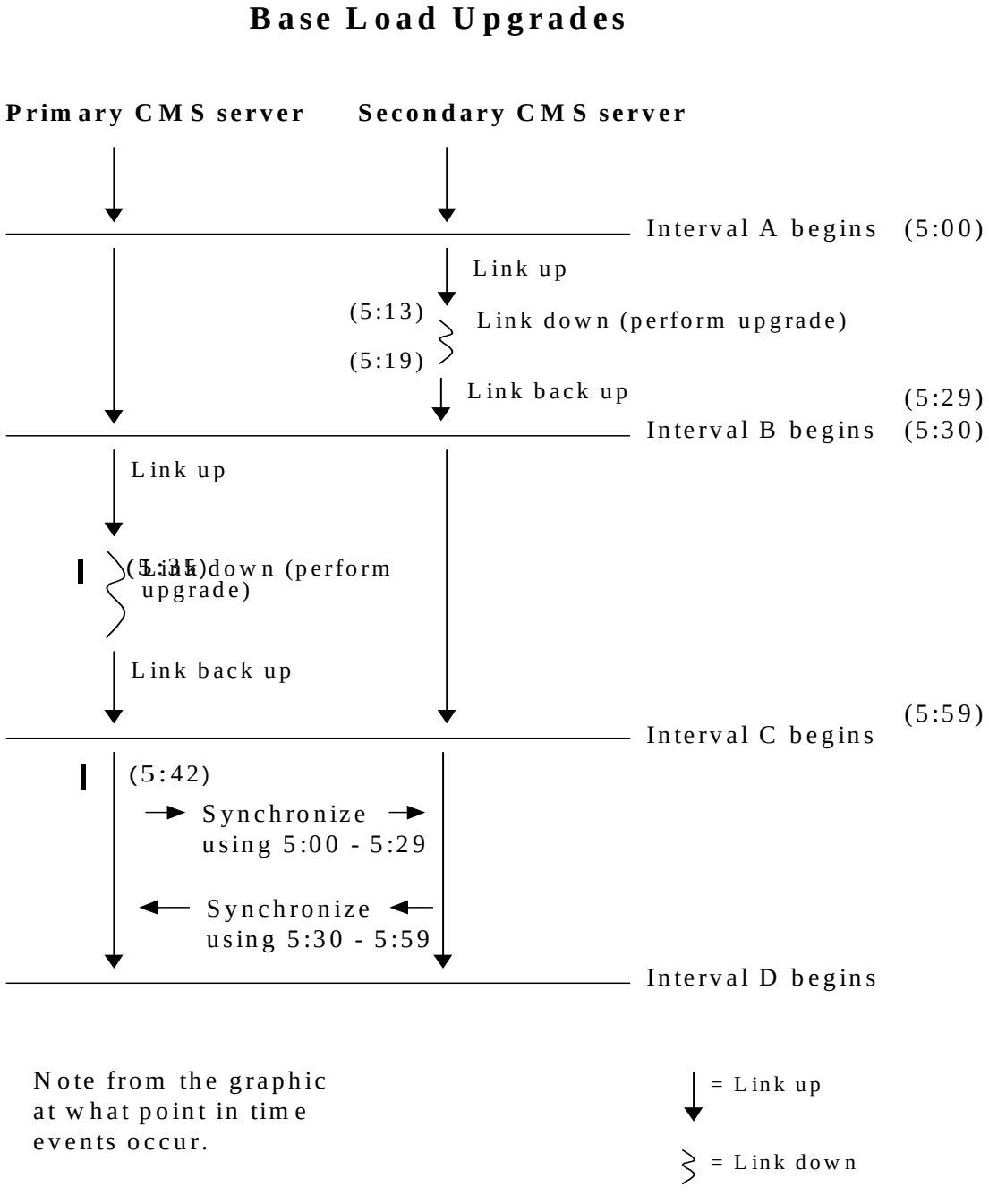
How do I know when I should perform a server switch-over from the Primary to the Secondary HA server? Server switch-overs are not recommended for system outages of realtively brief duration. However, it is the responsiblity of each CMS customer to establish their own criteria as to exactly what constitutes an unacceptable amount of time during which call data remains unavailable for analysis and review.

Appendix G: CMS Base Load Upgrade Procedure for High Availability Systems

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.

A conceptual illustration of a typical base load upgrade sequence for an HA system is depicted in the figure shown on page 2, and the steps for the procedure follow on page 3.

Conceptual depiction of the base load upgrade process for a CMS HA system.



Base Load Upgrade Procedure

Complete steps 1 through 5 not more than 24 hours before the base load upgrade:

CMS R3V8 HA Baseload Upgrade Procedure	✓
1. Verify the existing CMS version and load on the Primary and Secondary CMS servers. To do this, open a terminal window and enter: `pkginfo -x cms` The output will indicate the CMS version and base load number currently running on the system.	
2. Verify the free space available on the Primary and Secondary CMS servers (see "Verifying Free Space in the Root File System" in Chapter 3, CMS Upgrades and Migrations).	
3. Verify the free space available on the Primary and Secondary CMS servers (see "Verifying Free Space in the Root File System" in Chapter 3, CMS Upgrades and Migrations).	
4. Complete a cmsadm backup on the Primary and Secondary CMS servers. (see "Performing a CMSADM Backup" in Chapter 3, CMS Upgrades and Migrations).	
5. Complete a full maintenance backup on the Secondary CMS server. (see "Performing a Full Maintenance Backup (see "Performing a CMSADM Backup" in Chapter 3, CMS Upgrades and Migrations).	
6. Complete a full maintenance backup on the Primary CMS server. (see "Performing a CMSADM Backup" in Chapter 3, CMS Upgrades and Migrations).	
7. Turn off CMS on the Secondary CMS server. **Note the date and time** the CMS was turned off.	**Date/Time** _____
8. Remove CMS patches (as applicable) on the Secondary CMS server. (see "Removing CMS Patches" in Chapter 3, CMS Upgrades & Migrations).	
9. Remove the current CMS R3V8 load on the Secondary CMS server. (see "Removing the Current CMS Load" in Chapter 3, CMS Upgrades and Migrations).	
10. Install the Informix ILS 3.0 software (if not installed on the system). For details see "Installing Informix ILS 3.0" in Chapter 3, CMS Upgrades and Migrations).	
11. Install *Solaris* patches (if applicable) on the Secondary CMS server (see "Installing Solaris Patches" in Chapter 3, CMS Upgrades and Migrations).	
12. If a new version of the CMS Supplemental Services is required, install the software (see Upgrading CMS Supplemental Services, in Chapter 3, CMS Upgrades and Migrations).	

CMS R3V8 HA Baseload Upgrade Procedure	✓
13. Install the CMS R3V8.x load on the Secondary CMS server (see "Installing a New CMS Base Load" in Chapter 3, CMS Upgrades and Migrations).	
14. Install CMS patches (as applicable) on the Secondary CMS server (see "Installing CMS Patches" in Chapter 3, CMS Upgrades and Migrations).	
15. Turn CMS "on" on the Secondary CMS server, and verify that all the links come back up. **Note the date and time** when all the links come back up.	**Date/Time** _____
16. Wait for at least one interval of historical data to pass to allow data to be archived. (Use this time to ensure that the new load functions correctly before upgrading the Primary CMS server. Remember that you cannot synchronize the machines until they have the same software load.)	
17. If applicable, activate ECH on the Secondary CMS server.	
18. Stop CMS on the Primary CMS server. **Note the date and time** the CMS was turned off.	**Date/Time** _____
19. Remove CMS patches (as applicable) on the Primary CMS server (see "Removing CMS Patches" in Chapter 3, CMS Upgrades and Migrations).	
20. Remove the CMS R3V8 load on the Primary CMS server (see "Removing the Current CMS Load" in Chapter 3, CMS Upgrades and Migrations).	
21. Install the Informix ILS 3.0 software (if not installed on the system). For details see "Installing Informix ILS 3.0" in Chapter 3, CMS Upgrades and Migrations).	
22. Install *Solaris* patches on the Primary CMS server (see "Installing Solaris Patches" in Chapter 3, CMS Upgrades and Migrations).	
23. If a new version of the CMS Supplemental Services is required, install the software (see Upgrading CMS Supplemental Services, in Chapter 3, CMS Upgrades and Migrations).	
24. Install the CMS R3V8.x load on the Primary CMS server (see "Installing a New CMS Base Load" in Chapter 3, CMS Upgrades and Migrations).	
25. Install CMS patches (as applicable) on the Primary CMS server (see "Installing CMS Patches" in Chapter 3, CMS Upgrades & Migrations).	
26. Turn CMS "on" on the Primary CMS server, and verify all the links come back up. **Note the date and time** all the links come back up.	**Date/Time** _____
27. Wait for an interval to complete and be archived.	
28. Complete a full maintenance backup on the Secondary CMS server. (Refer to CMS Upgrades & Migrations, p. 3-6).	

CMS R3V8 HA Baseload Upgrade Procedure	✓
29. Complete a full maintenance backup on the Primary CMS server. (Refer to CMS Upgrades & Migrations, p. 3-6).	
30. On the Secondary CMS server, restore the historical data from the Primary CMS server using the time ***at the beginning*** of the interval during which the interruption occurred (for e.g., 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 (continuing with our example, if the link went down at 5:13 and came back up at 5.19, enter 5:29 as the stop time).	
31. On the Primary CMS server, restore the historical data from the Secondary CMS server using the time at the beginning of the interval during which the interruption occurred. Enter the stop time for the end of the interval during which the interruption occurred. Continuing with the example introduced in the last step, if the interruption on the Primary 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.	
32. Complete a cmsadm backup on the Secondary CMS server (see CMS Upgrades and Migrations, p. 3-3).	
33. Complete a cmsadm backup on the Primary CMS server (see CMS Upgrades and Migrations, p. 3-3).	

Index

A

ACD
- administration data . . . C-2
- Call Processing software . . . 1-3
- dual link . . . F-1
- link failures . . . 1-5

Agent Groups . . . 3-6
Agent Skills, changing . . . 3-2
Agent Trace, modifying . . . 3-1
Automatic Scripts . . . 3-10

B

Backup . . . 4-1
- cmsadm . . . 1-4
- files excluded from a CMSADM backup . . . B-1
- labels . . . A-1

Backup & Restore procedure . . . A-1

C

Call Work Codes, updating . . . 3-2
C-LAN . . . 1-3
CMS
- software failures . . . 1-6

CMS Server . . . P-2
- backup . . . A-1
- capabilities . . . 1-1
- changing timetables . . . 3-18
- data collected . . . F-1
- failure . . . E-1
- hardware failures . . . 1-5
- maintenance . . . 1-6, 2-2
- manual synchronization . . . 1-4
- operations on both . . . 2-5
- primary . . . 2-1
- running timetables . . . 3-17
- secondary . . . 2-1
- synchronizing . . . 3-12
- unscheduled outage . . . 4-1, 4-2
- upgrades . . . 1-6

CMS System Administration Data . . . C-1
CMS Users
- new . . . 3-20
- removing . . . 3-20
- setting user passwords . . . 3-21

cmsadm Backup . . . 1-4
Custom Reports . . . 3-2
Customer Care Helpline . . . P-2

D

Data Availability . . . 1-5
Data Collection
- synchronizing CMS servers . . . 3-12
- turned off . . . 2-8
- turned on . . . 3-9

Data Storage Allocation . . . 3-9
DEFINITY . . . 1-1, 2-2, F-1
Designer Reports . . . 3-3
Dictionary . . . 3-4, 3-5
Documents . . . P-2
Dual ACD Links . . . 1-3, F-1

E

Enhancements . . . 1-4
External Call History (ECH) . . . 1-5, 2-1

F

Forecast Data Storage Allocation . . . 3-9
Forecasting
- administration of report data . . . 3-9

Frequently Asked Questions . . . F-1

H

Hardware
- failures . . . 1-5
- platforms . . . 1-4

Helpline . . . P-2
High Availability, defined . . . 1-1, F-1
Historical Data . . . C-3

I

IL Number . . . P-3
Incremental backup . . . A-1
INFORMIX . . . C-1
Interactive Scripts . . . 3-10
Internet Call Center . . . 2-1

M

Main Menu . . . 3-10
Maintenance Restores, non-disruptive . . . 1-4
Manually synchronizing servers . . . 1-4

O

Operations
- both CMS servers . . . 2-5
- data collection off . . . 2-8

P

Platforms, supported 1-4, F-1
Prerequisites P-1
Primary CMS Server 2-1
  failure E-1
  unscheduled outage 4-1
Publications Center P-2

R

R3 migration, non-disruptive 1-5
R3V8 Enhancements 1-4
Recovery Kit 2-3
Related documents P-2
Reports
  custom 3-2
  designer 3-3
Restore 4-1

S

Secondary CMS Server 2-1
  failure E-1
  unscheduled outage 4-2
Service contract P-3
Shortcuts 3-10
Software
  failures 1-6
  Internet Call Center 2-1
  shipped with CMS 2-3
Split/Skill Call Profile 3-11
Sun Enterprise 3000 . . . . . P-2
Sun Enterprise 3500 . . . . . P-2
Supported platforms 1-4, F-1
Synchronization
  backup tapes 4-1
  data 2-2
  Main Menu additions 3-10

T

TCP/IP 1-3
Technical Service Center P-2
Timetables 2-1
  changing server information 3-18
  running on servers 3-17
Troubleshooting E-1
TSC P-2

U

Ultra5 . . . . . P-2
unscheduled 4-1
Updating
  Agent Skills 3-2
  Call Work Codes 3-2
Upgrades
  base load 3-1

V

VDN Call Profile Administration 3-21
Visual Vectors 3-22