Upgrading Avaya Call Management System

Release 21.0
Issue 2
June 2024

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document describes how to upgrade from Avaya Call Management System (CMS) Release R16.x or later to the latest release. To upgrade to from a previous release to the latest release, use the CMS Upgrade Express (CUE) upgrade process to perform a full software or platform upgrade.

This document is intended for implementation engineers and system administrators.

Change history

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

Issue	Date	Summary of changes
2	Late June 2024	• Cleaned up the remaining outdated content and revised content throughout the document to provide up-to-date information. • Simplified various procedures for clarity. • Removed references to the document *Planning for Avaya Call Management System Upgrades*. **Note:** All relevant preparation and post-upgrade information is already covered in this *Upgrading Avaya Call Management System*. After Release 21.0, *Planning for Avaya Call Management System Upgrades* will no longer be updated and will be considered obsolete.
1	Early June 2024	• Revised outdated interoperability and hardware information. • Various edits and formatting fixes. • Minor structural updates.

Chapter 2: Preparing for the upgrade

Use the information in this chapter to help you prepare for an upgrade. Perform the tasks outlined in this chapter before starting the upgrade.

Important:

All relevant preparation and post-upgrade information is covered in this document. Therefore, *Planning for Avaya Call Management System Upgrades* will no longer be updated and will be considered obsolete after Release 21.0.

Supported upgrade scenarios

CMS supports the following upgrade scenarios:

- Software Upgrades: Upgrade from an older CMS software release and retain the same hardware server or VMware server. You will back up the customer data, use software discs and a CMS OVA file to install the new Linux OS and CMS software, and then migrate the customer data.
- Platform Upgrades: Upgrade from an older CMS software release and install a new customer-provided VMware server or an Avaya Solutions Platform 130 Appliance VMware server. You will back up the customer data, use a CMS OVA file to install the new Linux OS and CMS software, and then migrate the customer data onto the new software release.
- Base Load Upgrades: Simplified upgrade process, which is available for CMS upgrades within the same minor release and other approved scenarios. You will use a software disc or a CMS ISO image file to install the new Linux OS and CMS software.

Software upgrades

The software upgrade process reuses existing CMS hardware that can support the new CMS software. The following server models are currently supported:

- Avaya Solutions Platform 130 Appliance VMware servers
- Customer-provided VMware servers
- Customer-provided Amazon Web Services (AWS) servers
- Customer-provided Google Cloud Platform (GCP) servers

Platform upgrades

CMS Release 21.0 supports platform upgrades from CMS Releases 16.x and later.

Note:

Contact your Avaya account team if you need to upgrade from CMS releases older than 16.x.

Base load upgrades

You can perform a base load upgrade within a CMS release or for other approved scenarios. For more information about base load upgrades, see *Avaya Call Management System Base Load Upgrade*.

You must perform a full software or platform upgrade from Release 20.0 or an earlier release to Release 21.0.

Software upgrade media

When upgrading a customer-provided or Avaya Solutions Platform VMware server, download the CMS OVA file and the upgrade ISO file to do the upgrade.

Platform upgrade media and upgrade process

When you upgrade your system by installing a new customer-provided or Avaya Solutions Platform VMware server, you do not receive an upgrade kit. You must install the new system as described in *Deploying Avaya Call Management System*. As part of the new installation, download the latest CMS file. After deploying the new system, migrate customer data onto it.

Updating CMS user IDs before an upgrade

CMS user IDs cannot contain diacritical, accented, special characters, punctuation, or blanks (for example, á, ñ, ç, |, ©, _). Older CMS releases might have user IDs that were administered with these unsupported characters. Before starting an upgrade, change the required CMS user IDs to only use alphanumeric characters and keep the length of these user IDs between 3 to 8 characters. For example, if you have “Dave_15” as a user ID, change it to “Dave15”. You cannot change or delete user IDs after the upgrade, so you must change them before the upgrade.

Backing up the old system

Move data from the old system to the new system as part of a software or platform upgrade. Tape drives are no longer supported with many of the latest CMS releases and backups to USB storage devices are not supported on VMware deployments. Therefore, use the NFS backup option when upgrading to a new CMS release.

A CMSADM backup is usually done the night before the upgrade. A full maintenance backup is usually scheduled to run overnight the night before the upgrade. However, if an incremental backup is not being done, run the full maintenance backup just before the upgrade. For information about backing up your data, see the CMSADM backup procedures in *Maintaining and Troubleshooting Avaya Call Management System*.

Collecting third-party and custom software

If third-party software, custom software, or other Avaya products are installed, gather that software so it will be available for installation after the upgrade. This can include software such as Operational Analyst or information about pseudo-ACDs. After the upgrade, reinstall the software.

Note:

Database changes might affect third-party software. For more information about database changes, see *Avaya Call Management System Database Items and Calculations* and *Avaya Call Management System Call History Interface*.

Related links

Installing and administering unpreserved third-party and custom software on page 24

Troubleshooting and escalation

About this task

Use these high-level steps if problems occur during the upgrade process.

Procedure

1. Escalate the problem through normal channels.
2. Inspect the upgrade log file that is located at `/var/log/cvuelog`.
3. If the problem persists, shut down the virtual system, reconnect the ACD links to the old system, and bring the old system back up under the old CMS load.

Communication Manager software and link compatibility

CMS supports Communication Manager releases, 7.x, 8.x, and 10.x. The CMS upgrade extract tool detects any incompatibility with ACD systems. If required, upgrade your ACD (for example, Communication Manager). You will need to enter a hostname or IP address and TCP port before the upgrade continues.

Note:

If the hostname or IP address and TCP port information is not known during the CMS upgrade, you can enter fictitious information to get through the upgrade. The Communication Manager links do not become active until you update the Communication Manager setup information with accurate information.

Encryption of personal data being exchanged with the Communication Manager system is a standard feature on CMS. To take advantage of personal data encryption, administer Communication Manager Release 8.1.2 or later on CMS and administer CMS 19.1 or later on the Communication Manager system.

Customization and software configuration

The upgrade process does not preserve third-party software packages and customizations. You must collect, reinstall, recompile, and reconfigure any non-standard CMS software after the upgrade is completed.

The customer data that is copied during the upgrade process includes the following:

- User login IDs and passwords
- System name and IP address
- Printer administration
- CMS administration
- CMS setup
- Feature installation

For a complete list of the files copied during the upgrade, see the `/var/log/cvuelog` file after the upgrade is complete. A copy of the old system’s `/etc/fstab` file is saved in the `cvuelog` file.

Checking for ACD 1

About this task

To perform an upgrade, ACD 1 must be administered. Use this procedure to check if it is administered.

Procedure

1. Log in to CMS Supervisor.
2. Under **System Setup**, view the list of administered ACDs.
    - If ACD 1 exists, continue with Recording storage interval data on page 15.
    - If ACD 1 does not exist, continue with the next step.
3. To add a temporary ACD 1:
    a. Run the `cmsadm` command.

    b. Enter `1` to select the **`acd_create`** option.

    This command adds the first unassigned ACD, which is ACD 1.

    c. Enter the switch name and switch model.

    d. Enable vectoring and disconnect supervision.

    e. Enter `1` for the local port and `1` for the remote port.

    f. Select TCP/IP for the link device.

    You can use an invalid IP address because the temporary ACD will be deleted after the upgrade.

    g. For the remaining options, use the default or minimum values.

Recording information about the old system

Record information from the old system to use when you provision the new system.

Use the blank forms in the appendix to record this information. See Blank data forms on page 45.

Accessing ACD information

About this task

CMS supports the following ACD types:

- Avaya Aura® Communication Manager
- Avaya Contact Center – Extended Capacity Routing Core

You can access a list of ACDs administered on the old CMS and then view the details for a specific ACD instance (switch).

Procedure

1. Using an administered CMS user ID, run `su - root` to log in with root privileges.
2. Run the `cmssvc` command.

   The CMS Services menu is displayed.
3. Enter the option number for `swinfo`.

   A list of administered ACDs is displayed. For example:

```
Select an ACD
    1)acd_number_1
    2)acd_number_2
Enter choice (1-2) or q to quit:
```

4. Enter the number that corresponds to the ACD for which you want information.

   Switch administration data for the selected ACD is displayed. For example:

```
Switch administration for acd 1:
    Switch name: em01
    Switch model: Communication Mgr 8.x
    Vectoring: y
    Expert Agent Selection: y
    Local port: 1
    Remote port: 1
    Link: TCP/IP em01 5001Switch administration for acd 1:
```

5. Repeat this procedure for each ACD that was administered on the old system.

Viewing authorizations

About this task

Use this procedure to display the current CMS authorizations.

Feature authorizations are controlled by a license file installed on the WebLM server. Record the feature authorizations on the old system to ensure that you have access to the same features on the upgraded system.

Procedure

1. Run the `cmssvc` command.

   The CMS Services menu is displayed.
2. Select the `auth_display` option.

   Current authorizations for CMS features and capacities are displayed. The options for authorization status are as follows:

   - Authorized: The feature is purchased and authorization is turned on.
   - Not authorized: The feature is not purchased or authorization is not turned on.
   - Installed: The feature is authorized and the software to support the feature is installed. For External Call History, the display indicates if the feature is on or off.

3. Use the blank form CMS authorizations on page 45 to record the current authorizations.

Activating the license for a CMS server

About this task

Each CMS deployment must have its own license file on the WebLM server. Enterprise licensing is not supported. Therefore, multiple CMS deployments cannot share one license file.

Before you begin

Get the following information:

- SAP order number
- License activation code (LAC)
- WebLM server host ID

✱ **Note:**

The SAP order number and the WebLM server host ID must be listed under the same Company ID.

Procedure

1. In a browser window, navigate to the PLDS website at https://plds.avaya.com.
2. Log in to PLDS using your customer ID and password.
3. Navigate to **Assets** > **View Entitlements**.
4. Search for your license entitlement using one of the following criteria:
    - SAP order number
    - Sold to number
    - License activation code

    You can also use **Advanced Search** to find a license entitlement.
5. Click **Search Entitlements**.

    PLDS displays the known license entitlements based on the search criteria.
6. For the customer entitlement record, click **Options** > **Activate**.

    PLDS displays a list of possible entitlements.
7. Select the entitlement for the CMS release you are installing or upgrading to.
8. Click **Activate**.

    PLDS displays the Search License Hosts page. The available license hosts for the Company ID are displayed.
9. Select one of the displayed license hosts or create a new host by clicking **Add a License Host**.
10. Click **Next**.

    PLDS displays a registration summary.

11. Click **Next**.

    PLDS displays the Activate Entitlements page.
12. Select the quantity of each entitlement you want to activate.
13. Click **Next**.
14. Add notes for the activation, if needed.
15. Click **Finish**.

Checking data storage allocation parameters

About this task

Use this procedure to check the data storage allocation parameters for each ACD on the old system.

Procedure

1. Log in to CMS and run the `cms` command to access the main menu.
2. Select **System Setup** and then press `Enter`.
3. From the menu, navigate to **Data Storage Allocation** and then press `Enter`.
4. Press `F3` (Commands) to display the print menu.

   Ensure that you print the window and save the printout. If you cannot print the record, use a blank form to record the information.
5. Press `F3` and navigate to **Options** > **Current ACD** to select another ACD.
6. Repeat this procedure for each ACD.

Checking the storage interval size

About this task

Use this procedure to check the storage interval size for each ACD on the old system.

Procedure

1. Log in to CMS and run the `cms` command to access the main menu.
2. Select **System Setup** and then press `Enter`.
3. From the menu, navigate to **Storage Intervals** and then press `Enter`.
4. Press `F3` (Commands) to display the print menu.

   Ensure that you print the window and save the printout. If you cannot print the record, use the blank form Storage intervals on page 48 to record the information.
5. Press `F3` and navigate to **Options** > **Current ACD** to select another ACD.
6. Repeat this procedure for each ACD.

Recording master ACD clock synchronization information

About this task

Preserve the master clock ACD information so that you can reconfigure it after the upgrade.

Procedure

1. Log in to CMS.
2. Select **System Setup** > **CMS State** to display the Master ACD clock information.
3. Record the ACD displayed in the **Master ACD for clock synchronization** field.

   ```
   /etc/sysconfig/network-scripts/ifcfg-eth*
   ```

Administering printers

About this task

Use these guidelines to administer printers on Linux.

Procedure

1. Run `lpstat -t | more` to display a list of administered printers.
2. Based on the displayed printer names, run `lpstat -p <name> -l | more` to display the printer type and speed for each of the printers.
3. Navigate to **Maintenance** > **Backup/Restore Devices** to display the current default printer device.

   Record that information to administer on the new system.

Recording storage interval data

About this task

During an upgrade, some storage interval data is not preserved. The majority of the storage interval data is preserved in the `storage.def` file. However, the information for the data summarizing time, switch time zone offset, and master clock ACD are not part of the `storage.def` file.

Use this procedure to record information so you can reconfigure it after the upgrade.

Procedure

1. Log in to CMS and run the `cms` command to access the main menu.
2. Select **System Setup** > **CMS State** to display the Master ACD clock information.
3. Record the ACD displayed in the **Master ACD for clock synchronization** field.
4. For each ACD, select **System Setup** > **Storage Intervals** to display the storage interval data for the ACD.
5. Record the **Data summarizing time** and **Switch time zone offset** entries.

You can print the window to record the data.

6. Repeat steps 4 and 5 for each ACD.

Recording dual IP setup information

About this task

Use this procedure to record the setup information for a dual IP deployment.

Procedure

1. Log in to the CMS server with root privileges.
2. Run `cmssvc` to display the CMS Services menu.
3. Enter the number corresponding to the **`swinfo`** option.
4. Record the dual IP information for each ACD.

Chapter 3: Extracting data from the old system

To minimize the time that CMS is out-of-service during the upgrade, you can extract your customer data while CMS is operating. After starting the extract process, do not make any administrative changes.

Use a network mount point as the extract device. Ensure that you extract customer data from the old system before you copy and activate it on the new system.

Related links

Backing up the old system on page 9

Preparing to extract data to a network mount point

CMS supports backups to network mount points on all deployments.

As a system administrator, you are responsible for the proper configuration of network mount points and connectivity to the CMS server. Ensure that the CMS server detects your network mount point and that you can perform read and write operations to or from the mount point. Determine if any security violations will occur before creating shared mount points and allowing other systems on the network to access them.

When using NFS mounted directories:

- The NFS mount point must be accessible from the CMS server.
- The directory path used when administering an NFS backup device must exist on the NFS server.

The following procedures provide basic information about configuring the NFS server and the CMS server to support upgrade extracts to NFS servers.

Performing the NFS server configuration

About this task

This procedure describes the configuration you perform on the NFS server, which must be a separate, non-CMS, customer-provided Linux computer.

Procedure

1. On the NFS server, run `mkdir /network_server_mt_pt_dir` to create the network mount point.
2. To set permissions, run the following:

   ```
   chmod 755 /network_server_mt_pt_dir
   chown nobody:nobody /network_server_mt_pt_dir
   ```

   For example:

   ```
   chmod 755 /CUE_NFS_dir
   chown nobody:nobody /CUE_NFS_dir
   ```

   Later, if you see a “Permission denied” message and cannot write to the network mount point on the CMS server, run `chown nfsnobody:nfsnobody /network_server_mt_pt_dir` to set the owner and group to **`nfsnobody`**.
3. Do the following to provide access to other systems:
   a. Run the `vi /etc/exports` command.
   b. Run `/network_server_mt_pt_dir <CMS_FQDN>(rw,sync)` to append the network mount point information to the bottom of the file.

      For example: `/CUE_NFS_dirtrapper1.dr.avaya.com(rw,sync)`
   c. Save the file.
4. Do the following to configure NFS and portmap to start after a reboot:
   a. Using an administered CMS user ID, run `su - root` to log in with root privileges.
   b. Run `ntsysv` at the command line prompt.
   c. Review the list and ensure that the NFS and portmap options are selected.
   d. Press `Tab` to highlight **OK** and then press `Enter`.
5. Do one of the following:
   - If the NFS service is not running, run the `/etc/init.d/nfs start` command to start it.
   - If the NFS service is running, run the `/etc/init.d/nfs restart` command to restart it.
6. Run `service nfs status` to verify that the network service is running.

Performing the CMS server configuration

About this task

This procedure describes the CMS server configuration required to support data extracts to a network mount point.

Procedure

1. Run `mkdir /CUE_extract_dir` to create the network mount point directory.
2. To mount the NFS server, run the following command on a single line:

   ```
   mount -F nfs <network_server_ip_address>:/network_server_mt_pt_dir /
   CUE_extract_dir
   ```

   For example:

   ```
   mount -F nfs xxx.xxx.xxx.xxx:/CUE_NFS_dir/CUE_extract_dir
   ```
3. Run `cd /CUE_extract_dir` to switch to the network server mount point directory.
4. Run `ls -l` to list the contents of the network server mount point directory.
5. Ensure that there is adequate space on the NFS server to extract the CMS upgrade data.

   The `cvue_extract` process shows the space needed for the extracted data after all the extract information is collected. If there is insufficient space, the amount of available space and required space are displayed.
6. **(Optional)** To unmount a network server mount point directory, run the `unmount /CUE_extract_dir` command.

Extracting customer data

About this task

Use this procedure to extract customer data from the old system before you copy and activate it on the new system.

Before you begin

- Ensure that you performed the required preparation to extract data to a network mount point.
- To upgrade a VMware system, download the CMS upgrade ISO file from the Avaya Support site.

Procedure

1. To begin the extract process, log in to the CMS server with root privileges.
2. Copy the CMS upgrade ISO file to the CMS server and run the following command to mount the ISO file:

   ```
   cd /
   mount <UpgradeISOPath> /mnt
   ```

   Tip:

   If the mount fails, you can run the following commands:

   ```
   cd /
   unmount /mnt
   mount <UpgradeISOPath> /mnt
   ```

3. Run `cd /mnt` to switch to the mount location.
4. Run `./cvue_extract` to start the extract process.

   The extract process verifies whether CMS supports the platform you are upgrading. If the platform is not supported, a warning such as the following is displayed:

   ```
   ***WARNING***
   You are upgrading from a hardware platform that is not supported by CMS. Do not
   continue if you do not have the proper platform for upgrade available.
   Do you want to continue? (y or n) :
   ```
5. Enter `y` to continue with the upgrade or `n` to stop the upgrade until you have the correct hardware ready.

   Proceed to the next step if you are continuing with the upgrade.
6. Review the extract process output to ensure that the CMS converter tool was run successfully.

   Information such as the following is displayed:

   ```
   Continuing with CMS Upgrade Express ...
   Admin data will be saved
   /var/tmp/new/adminsave/cmsadmin.saved
   Converter completed successfully.
   ```
7. Continue reviewing the extract process output to check if ACD 1 is administered.
   - If ACD 1 is administered, the extract process continues.
   - If ACD 1 is not administered, you see an error message such as the following:

     ```
     ERROR:
     ACD 1 is currently administered as a skipped ACD.
     CUE cannot upgrade when ACD 1 is a skipped ACD.
     Please run cmsadm, add a temporary ACD 1, then run
     "./cvue_extract" again.
     #
     ```

     For information about adding a temporary ACD 1, see Checking for ACD 1 on page 11 and then go back to step 4 to restart the extract process.
8. If required, upgrade your ACD system (for example, Communication Manager) when you upgrade CMS.

   The extract process verifies each ACD to determine if any of the ACDs are administered with an unsupported switch model.
   - If you have an unsupported switch model, enter information about the upgraded switch as indicated in steps 9 to 13.
   - If this CMS release supports all the ACDs, the extract process continues as indicated in step 14.
9. Enter the upgraded switch model for the ACD.

   If no other ACDs are administered with an unsupported switch model, proceed to the next step.

10. Enter the hostname or IP address of the switch.

    A message similar to the following is displayed:

    ```
    You have entered the following TCP/IP information for <acd_name> (ACD <acd
    number>):
    *************************************
    Host name or IP address: <host_name or IP_address>
    *************************************

    If you would like to make changes to the entry above,
    enter choice (y or n) (default: n):
    ```

11. Do one of the following:

    - If the entry is correct, press `Enter` to proceed with the extract process.
    - If the assignment is not correct, enter `y` to return to the previous step.

12. When prompted, enter the switch TCP port number.

    A message such as the following is displayed:

    ```
    You have entered the following TCP/IP information for <acd_name> (ACD <acd
    number>):
    *************************************
    TCP Port Number: <port_number>
    *************************************

    If you would like to make changes to the entry above,
    enter choice (y or n) (default: n):
    ```

13. Do one the following:

    - If you want to make changes to the entry, type `y` and then repeat the previous step.
    - If the entry is correct, press `Enter` to proceed.

      If there are more ACDs to be converted to TCP/IP, you are prompted to configure them as indicated in step 10. Otherwise, the extract process continues.

14. Wait for the extraction of the administration files to be completed.

    The extraction might take a few minutes. When it is completed, you see a message such as the following:

    ```
    NOTE: Be sure to review the cvuelog for any files
    to be merged manually in the upgraded system.
    ```

15. Review the messages that are displayed as the extract process continues.

16. When prompted, select the extract device type.

    You should be using a network mount point to extract data. Note that tape drives are no longer supported with the latest CMS releases and USB storage devices are not supported on VMware deployments.

17. Enter the extract device path when prompted.

    When using a network mount point, the extract device path must exist on the CMS server and must be mounted. If the network mount point does not exist or is not mounted, the extract will fail.

18. Continue reviewing the messages displayed.

    Ensure that the extract process writes the administration data to the extract device. A message such as the following is displayed:

    ```
    Admin data will be saved to /storage/cue/cvue_extract.tar

    manual_merge/ manual_merge/var/
    . . .
    . . .
    var/spool/cron/
    var/yp/
    Extract complete.
    The cvue_extract process is complete.
    ```

19. Enter the following commands to verify that the directory contains upgrade scripts.

    ```
    cd /var/tmp/new/adminsave/init.d
    ls -l
    ```

    If the scripts do not exist, check for free space on the server. Reboot the server and retry the extract.

20. Run `more /var/tmp/new/var/log/cvuelog` to display the temporary upgrade log file.

    Check for failure messages (FAIL) or other indications that the extract process was not successful.

    This file also contains a list of files that are copied to the new system. The list of files might be useful for later troubleshooting.

21. Run `ls -l /var/tmp/new/adminsave/cmsadmin.saved` and review the information displayed.

    If the files `setup.out`, `fp.install`, and `stor.def` do not exist or have a file size of zero, escalate though normal channels.

Chapter 4: Deploying a new CMS server

Use one of the following options when upgrading an existing CMS deployment:

- Software upgrade with an existing VMware server on page 23: If you are reusing an older customer-provided or Avaya Solutions Platform 130 Appliance VMware server that supports the new CMS release, redeploy the OVA on the existing server, reconfigure your settings, and then copy and activate customer administration data and other options.
- Platform upgrade on a new VMware server on page 24: If you need to replace existing hardware that is not supported on the new CMS release, deploy a new customer-provided or Avaya Solutions Platform 130 Appliance VMware system, and then copy and activate customer administration data and other options.

Ensure that you perform a backup of the old system if it is not yet done. For information about backing up customer data, see the CMSADM backup procedures in *Maintaining and Troubleshooting Avaya Call Management System*.

When deploying a new CMS server, turn on IDS, configure an encryption passphrase, set up licensing with a WebLM server, and enable Enhanced Access Security Gateway (EASG). These tasks are described in *Deploying Avaya Call Management System*.

Software upgrade with an existing VMware server

When upgrading CMS on an existing VMware server, perform the procedures in the following chapters of *Deploying Avaya Call Management System*:

- Deploying CMS software using an OVA file
- Configuring system features

After completing the procedures described in *Deploying Avaya Call Management System*, return to this *Upgrading Avaya Call Management System* document to complete the upgrade.

Platform upgrade on a new VMware server

When upgrading CMS on a new VMware server installation, perform the procedures in the following chapters of *Deploying Avaya Call Management System*:

- Planning an OVA deployment
- Deploying CMS software using an OVA file
- Configuring system features

After completing the procedures described in *Deploying Avaya Call Management System*, return to this *Upgrading Avaya Call Management System* document to complete the upgrade.

Installing and administering unpreserved third-party and custom software

After the upgrade, install software that was not preserved and administer any new features or services. The following is a list of these features and services:

- Network printers.
- Pseudo-ACDs - These must be added and data must be migrated from the old system.
- Applications such as workforce management software.
- Wallboards.
- Mounted file systems that were in the `/etc/fstab` file before the upgrade.

  Check the copy of the file saved in `/var/log/cvuelog` and verify that your new configuration is correct.
- Common Desktop Environment options such as screen layout and password protection.
- EASG.

Ensure that you also do the following:

- Add, change, or remove ACDs.
- Add Supervisor logins.
- Install new feature packages (if purchased).
- Change authorizations.
- Update security options such as `rsh` and `rlogin`.

Chapter 5: Finalizing the upgrade

After deploying the new server, mount the NFS. You can then copy and activate customer data. This chapter also provides information about turning on CMS and other tasks for finalizing the upgrade.

Mounting an NFS mount point

About this task

After deploying the new server, mount the extract device. Ensure that data can be written to and read from the network mount point extract path.

Procedure

1. On the CMS server, run `mkdir /CUE_extract_dir` to create the NFS mount point.
2. Run the `ifconfig -a` command.

   An output similar to the following is displayed:

```
eth0    Link encap:Ethernet HWaddr 90:B1:1C:55:21:4B
inet addr:135.9.131.127 Bcast:135.9.131.255 Mask:255.255.255.0
inet6 addr: fe80::92b1:1cff:fe55:214b/64 Scope:Link UP BROADCAST RUNNING
MULTICAST MTU:1500 Metric:1
RX packets:3108896 errors:0 dropped:0 overruns:0 frame:0 TX packets:296988
errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000
RX bytes:713780687 (680.7 MiB) TX bytes:36371556 (34.6 MiB)
Interrupt:35

eth1    Link encap:Ethernet HWaddr 90:B1:1C:55:21:4C BROADCAST MULTICAST MTU:1500
Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0
dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:38

eth2    Link encap:Ethernet HWaddr 90:B1:1C:55:21:4D BROADCAST MULTICAST MTU:1500
Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0
dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:34

eth3    Link encap:Ethernet HWaddr 90:B1:1C:55:21:4E BROADCAST MULTICAST MTU:1500
Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0
dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

```
Interrupt:36

lo    Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:75254 errors:0 dropped:0 overruns:0 frame:0 TX packets:75254 errors:0
dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0
RX bytes:5954970 (5.6 MiB) TX bytes:5954970 (5.6 MiB)
```

3. Run `ping route_ip` and verify that the network router for the CMS server responds.
4. Run `ping nfs_server_ip_address` and verify that the network server responds.
5. To mount the network server, run the following command on a single line:

   ```
   mount -t nfs <network_server_ip_address>:/network_server_mt_pt_dir/CUE_extract_dir
   ```

   Important:

   The `network_server_mt_pt_dir` must be the same mount point created when you extracted data using the `cvue_extract` process.
6. Run `cd /CUE_extract_dir` to switch to the network server mount point directory.
7. Run `ls -l` to list the contents of the network server mount point directory.

   Ensure that the `cvue_extract.tar` file is listed.

Related links

Extracting customer data on page 19

Copying customer data

About this task

Use this procedure to copy customer data from the upgrade backup device onto the new system.

Before you begin

- Mount the extract device that you used for the `cvue_extract` process.
- If you are upgrading a VMware system, download the CMS upgrade ISO file from the Avaya Support website.

Procedure

1. To begin the copying process, log in to the CMS server with root privileges.
2. Copy the CMS upgrade ISO file to the CMS server and run the following command to mount the ISO file:

   ```
   cd /
   mount <UpgradeISOPath> /mnt
   ```

Tip:

If the mount fails, you can run the following commands:

```
cd /
unmount /mnt
mount <UpgradeISOPath> /mnt
```

3. Run `cd /mnt` to switch to the mount location.
4. Run the `./cvue_copy` command.
5. When prompted, specify the extract device type.
6. Enter the path where the `cvue_extract.tar` extract file is located.

   Ensure that the path is the same as the one used in the **`cvue_extract`** process. For example:`/CUE_extract_dir`.
7. Review the messages displayed as the copy process progresses.

   When the customer files are copied, a message such as the following is displayed:

   ```
   . . .
   . . .
   var/spool/cron/
   var/yp/
   <timestamp>:./cvue_copy: Finished reading admin data from
   <filepath>cvue_extract.tar
   <timestamp>:./cvue_copy: The CUE Copy process is complete
   ```
8. Ensure that the server reboots when the **`cvue_copy`** process is completed.

   The server should reboot automatically to finish cleaning up configuration changes. If the server powers off instead of rebooting, power it on.

Next steps

Continue with Activating customer options on page 27.

Related links

Extracting customer data on page 19

Activating customer options

About this task

The amount of time required to activate customer options depends on the number of options, the number of ACDs, and other parameters.

Before you begin

- Ensure that the mount point used for backups is accessible.
- If you are upgrading a VMware system, download the CMS upgrade ISO file from the Avaya Support website.

Procedure

1. To begin the activation process, log in to the CMS server with root privileges.
2. Copy the CMS upgrade ISO file to the CMS server and run the following command to mount the ISO file:

   ```
   cd /
   mount <UpgradeISOPath> /mnt
   ```

   Tip:

   If the mount fails, you can run the following commands:

   ```
   cd /
   unmount /mnt
   mount <UpgradeISOPath> /mnt
   ```

3. Run `cd /mnt` to switch to the mount location.
4. Run the `./cvue_activate` command.
5. Run the `tail -f /var/log/cvuelog` command from the local console during the copy and activation process to view the upgrade log file.

   Tip:

   When you finish viewing the `/var/log/cvuelog` file, press `Delete` to break out of the command.

6. Review the messages displayed to verify if the process is successful.
   - If the copying is successful, CMS starts activating customer options. A message such as the following is displayed:

     ```
     Starting running scripts from /adminsave/init.d directory

     S00Sethostname Start Time -> <timestamp>
     S00Sethostname End Time -> <timestamp>
     . . .
     . . .
     ```

   - If the copying is not successful, you are prompted to run the **`cvue_copy`** process again. For more information about performing this copying process, see Copying customer data on page 26.
7. Verify the messages displayed to ensure that serial printers are readministered.

   After the upgrade, network printers must also be administered.
8. Enter the option for the type of backup device you are using.
9. **(Optional)** If the **`S21checkdevices`** check fails, ensure that the default backup path in the `/cms/db/cms.install` file is correct.

   This problem can occur because the default backup path in the `/cms/db/cms.install` file is a tape drive or the path does not exist. If this problem occurs, do the following:

   a. Make a note of the default backup device currently defined in the `/cms/db/cms.install` file and make a copy of the file.

   b. Modify the original file so the default backup device path is the mount point being used for the extract device.

   c. Save the file and exit the editor.

   d. Run the `./cvue_activate` script again.

10. Review the command output messages to ensure that the activation process is proceeding as expected.

    If the new system was deployed as described in the chapter Deploying a new CMS server on page 23, you should not see prompts about setting up WebLM, EASG, or the encryption passphrase. However, if you are prompted to provide this information, messages such as the following are displayed. Set up these options now or later.

    ```
    You are required to set the WebLM host name before proceeding.
    . . .
    . . .


    EASG User Access
    . . .
    . . .
    Would you like to enable Avaya EASG? (Recommended) [yes/no]:
    . . .
    . . .
    ```

11. Continue monitoring the messages displayed to ensure that CMS set is completed successfully.

    The following is an example of the output displayed:

    ```
    . . .
    . . .
    Customer CMS data successfully initialized <time stamp>
    .............................................
    Computing space requirements and dbspace availability.
    Setup completed successfully.
    S80cmssetup End Time -> <time stamp>
    . . .
    . . .
    ```

    Note:

    If you are looking at the `/var/log/cvuelog` file during CMS setup, ignore any messages about SQL database failure.

    CMS setup takes a few minutes to complete.

12. Ensure that the activation process is completed successfully.

    If script errors occurred or the activation process is not completed, see Recovering from failed installation scripts on page 30.

Recovering from failed installation scripts

An error message such as the following indicates that a failure occurred in one of the installation scripts:

```
ERROR[1]: FUNCTION S00Sethostname() FAILED at <time stamp>
script /adminsave/init.d/S00Sethostname failed
```

You can recover and continue with the upgrade by skipping the failed installation script. Any script that you skip during this part of the upgrade must be installed later using standard software installation procedures.

The following sections provide more information about installing skipped scripts and explain what to do if one of the scripts fails during the upgrade. When identifying the installation scripts, note that each script is numbered with a prefix (for example, S04) before the script name.

Getting started with scripts that can be skipped and installed later

About this task

The **cmsfeatpkg** installation scripts for CMS Feature Packages can be skipped during the upgrade. These scripts are used to install software or drivers. Any script that is skipped during the upgrade must be installed later. This procedure provides high-level information. For more detailed feature package installation information, see *Maintaining and Troubleshooting Avaya Call Management System*.

Procedure

1. Run the `cd /adminsave/init.d` command.
2. Run `mv <scriptname> /adminsave/`, where `<scriptname>` is the name of the script.
3. Run `cd /mnt` to switch to the mount location.
4. Run the `./cvue_activate` command.
5. Install the software package that you skipped before migrating customer data.

   After each script is run, a copy of the script is automatically moved to the directory `/adminsave/init.d.completed`.

Failures that require escalation

For the scripts listed in the following table, do not attempt to continue with the upgrade. Escalate the problem through normal channels.

Script name	Description
Sethostname	Sets the hostname.
sqlhosts	Sets up the SQL hosts file.
AdministerPrinters	Administers serial printers.
modifyfile	Restores CMS setup information.

Table continues…

Script name	Description
checkdevices	Checks for devices.
MigrateAlarmData	Migrates alarm data.
init_db	Initializes the database.
storage	Data storage allocation.
converter	Preserves CMS setup data.
cmssetup	CMS setup script.

Resolving failures that occur when adding features

About this task

If ECH is installed and pseudo-ACDs are also administered on the system, the restore process and the CMS upgrade process fail during the installation of the CMS feature packages (script **S81cmsfeatpkg**).

Use this procedure if the restore process or the CMS upgrade process fails when installing CMS feature packages.

Procedure

1. See `/var/log/cvuelog` for error messages.
2. Verify whether the script `/adminsave/init.d/S81cmsfeatpkg` exists.
3. If the script exists, open the file `/adminsave/cmsadmin.saved/fp.install` and search for any ACD entry that references `unnamed_acd`.
4. If the entry exists, make a copy of the original `fp.install` file.
5. Edit the `/adminsave/cmsadmin.saved/fp.install` file, and delete or comment out the `unnamed_acd` value.

   In the following example, the value to be commented out is 20,000:

   ```
   # Number of call segments to buffer for ACD unnamed_acd9:
   #20000
   ```
6. Save the modified file.
7. Run `./cvue_activate` again from the mounted directory.

Removing temporary ACD 1 (optional)

About this task

If you created a temporary ACD 1 during the upgrade process, use this procedure to remove the temporary ACD. Skip this procedure if you did not create a temporary ACD.

Procedure

1. Run the `cmsadm` command to display the CMS administration menu.
2. Enter `2` to select the **`acd_remove`** option.
3. Enter `ACD 1`.
4. When prompted, enter `y`.

Next steps

Continue with Turning on CMS on page 32.

Related links

Checking for ACD 1 on page 11
Extracting customer data on page 19

Turning on CMS

Procedure

1. Log in to the CMS server with root privileges.
2. Run `cmsadm` to display the CMS Administration menu.
3. Enter the number corresponding to the **`run_cms`** option.
4. Enter `1` to turn on CMS.

Next steps

Do one of the following depending on whether you are using the CMS Supervisor Web Client:

- If you are using CMS Supervisor, continue with Starting the CMS Supervisor Web Client on page 32.

  If you are not using CMS Supervisor, continue with Verifying that CMS is operating on page 33.

Starting the CMS Supervisor Web Client

Procedure

Run `cmsweb start` to start the CMS Supervisor Web Client.

Web client certificate management

A security certificate is required to encrypt communication between browsers and the CMS Supervisor web server. If CMS Supervisor is installed on the pre-upgrade system, the certificate will be copied over to the upgraded system during the software upgrades process. Run the `/opt/cmsweb/bin/showcrt.sh` command to view the Common Name used in this certificate.

The URL/Common Name is used to access the CMS Supervisor Web Client from your browser. If the URL is incorrect due to the network and host setup, obtain a new commercial certificate from your certificate authority.

If the certificate changes, restart CMS Supervisor to accept the changes. To restart the CMS Supervisor Web Client, run:

```
cmsweb stop
cmsweb start
```

Verifying that CMS is operating

Procedure

1. Log in to CMS and run the `cms` command to access the main menu.
2. Verify that the status of ACD links before the upgrade matches the status after the upgrade.

   For example, if a Communication Manager link was operating before the upgrade, ensure that it is still operating after the upgrade. If a link that should be operating is not, ensure that data collection is turned on.

Updating the ECH public key file

This procedure is only required if the upgraded CMS server sends records to an ECH system. Skip this procedure if records are not sent to ECH.

ECH uses a public key file on the CMS server. The information in the file gets put in the `authorized_keys` file in the Home directory of the SFTP user on the receiving ECH system. This file is located on the CMS server at:

```
URL/Common Name: cms163.avaya.com
/root/.ssh/id_rsa.pub
```

When the CMS server is upgraded through the CMS upgrade process on a Linux server, the upgrade changes the public key. Put the new public key file on the receiving ECH server so that the SFTP connection will work.

Updating the switch setup

About this task

The ACD switch might need to be upgraded to a new release when the CMS is upgraded. Verify switch setup for any ACDs where the switch model was changed. Perform this procedure if the switch model has changed.

Procedure

1. Check the switch links on the CMS main window.

   Perform the following steps if the links are not active.
2. Run the `cmssvc` command.
3. Enter the number corresponding to the **`swsetup`** option to check the administration of each ACD.

   CMS must be turned off to administer the ACDs. Remember to turn CMS on after setting up the ACDs.
4. Reconfigure the CMS version on the switch using the Feature Parameters form.

Updating dual IP information

About this task

Use this procedure to change the dual IP information for an ACD.

Procedure

1. Log in to the CMS server with root privileges.
2. Run the `cmssvc` command.
3. Enter the number corresponding to the **`run_cms`** option.
4. Enter `2` to turn off CMS.
5. Run the `cmssvc` command again.
6. Enter the number corresponding to the **`swsetup`** option.
7. Select the ACD you want to change.
8. At the secondary switch prompts, add the required information.
9. Review the data you entered. For example:

   ```
   Switch name: abc
   Switch model: Communication Mgr 8.x
   Local port: 1
   Remote port: 1
   Link: TCP/IP cmsvm10 5001
   Secondary link: TCP/IP cmsvm10 5002
   ```

10. If the data is correct, enter `y`.
11. Run `cmssvc` and enter the number corresponding to the **`run_cms`** option.
12. Enter `1` to turn on CMS.
13. Run `cmssvc` and enter the number corresponding to the **`swinfo`** option.

Updating storage interval data

About this task

During an upgrade, some storage interval data is not preserved. The majority of the storage interval data is preserved in the `storage.def` file. However, the information for the data summarizing time, switch time zone offset, and master clock ACD are not part of the `storage.def` file. Use this procedure to update the storage interval data that you noted in Recording storage interval data on page 15.

Procedure

1. Log in to CMS and run the `cms` command to access the main menu.
2. Select **System Setup** > **CMS State**.
3. Update the **Master ACD for clock synchronization** entry.
4. Save your update.
5. For each ACD, select **System Setup** > **Storage Intervals**.
6. Update the **Data summarizing time** and **Switch time zone offset** entries.
7. Save your update.
8. Repeat steps 5 to 7 for each ACD.
9. Log out of CMS.

Manual merge discrepancies

All files that must be manually merged are saved in the `/manual_merge` directory. If you do not see the files on the target machine, you can ignore the need for manual merges.

Removing the upgrade files

Procedure

1. Run the `cd /mnt` command.
2. Run `./cvue_cleanup` to begin the cleanup process.

   This process can take a few minutes depending on the number of files to remove. When the files are removed, you see a message indicating that the cleanup process is complete.

Next steps

Continue with Migrating customer data on page 36.

Migrating customer data

Use the information in the following sections to migrate data, including system administration data as well as agent and call center administration data.

Data migration considerations

Before migrating data, remember the following:

- Data must be backed up before it can be restored. To ensure the safety of your data, back up your system frequently.
- When migrating or restoring a non-LDAP user from a maintenance backup, if a “logid” (login ID) does not exist in `/etc/passwd`, the user is created as a new logid. If this occurs, the migration and restore logs contain entries such as the following:

  ```
  -    /cms/maint/r3mig/mig.log
  INFO: New UNIX user normusr1: name, room and telephone will not be
  migrated.
  -    /cms/maint/restore/rest.log Created UNIX login 'normusr1'.
  Warning: Name, Telephone, and Room will not be restored for
  normusr1.
  ```

  You must perform password administration for the new logid just like you would for a new user. For more information about setting user passwords, see *Administering Avaya Call Management System*.

Migrating system administration data

About this task

This procedure describes the process for migrating system administration data.

⚠ **Caution:**

Only perform this procedure once. Attempting to migrate system administration data more than once results in serious errors from which recovery might not be possible. Failure to heed this warning can result in irretrievably damaged data.

Procedure

1. If CMS is not turned on, do the following:
    a. Run `cmsadm` to display the system administration menu.
    b. Enter the number for the `run_cms` option.
    c. Enter `1` to turn on CMS.
2. Log in to CMS.
3. From the **CMS Main** menu, select **System Setup** > **CMS State** to put CMS into single-user mode.
4. Turn off data collection for all ACDs.
5. Insert the most recent full maintenance backup tape or mount the extract device.
6. From the **CMS Main** menu, select **System Setup** > **R3 Migrate Data**.
7. In the R3 Migrate Data window, do the following:
    a. In the **Device name** field, enter the extract device name.
    b. From **Data type**, select **System Administration data**.
    c. From **Specify ACD(s)**, select **All ACDs**.
8. Press `Enter` to access the action list in the top-right corner.
9. Select **Run** and press `Enter`.

    The migration progress is displayed.
10. Press `F3` and select the UNIX option to display the command line prompt.

    ✱ **Note:**

    After the migration is complete, you will receive a message if migration of any custom reports fail. Information about the failed reports are written to the `r3mig.log` file.
11. Run `pg /cms/migrate/r3mig.log` to display the customer migration log.
12. Verify the contents of the customer migration log and take any necessary corrective action.
13. Repeat steps 6 to 12 using the incremental backup media, if one was created.
14. Type `exit` to exit the command line window.

Migrating agent and call center administration data

Procedure

1. Verify that the most recent full maintenance backup is accessible by the extract device.
2. From the CMS main menu, select **System Setup** > **R3 Migrate Data**.
3. In the R3 Migrate Data window, do the following:
    a. In the **Device name** field, enter the extract device name.
    b. From **Data type**, select **Agent/Call Center Admin data**.
    c. From **Specify ACD(s)**, select **All ACDs**.
4. Press `Enter` to access the action list in the top-right corner.
5. Select **Run** and press `Enter`.

   The migration progress is displayed.
6. Turn on data collection for all ACDs.
7. Press `F3` and select the UNIX option to display the command line prompt.
8. Run `pg /cms/migrate/r3mig.log` to display the customer migration log.
9. Verify the contents of the customer migration log and take any necessary corrective action.
10. Repeat the previous steps using the incremental backup media, if one was created.
11. Type `exit` to exit the command line window.
12. Select **System Setup** > **CMS state** to put CMS into multi-user mode.

Configuring alarming options

Configure Alarm Origination Manager (AOM) as described in *Maintaining and Troubleshooting Avaya Call Management System*.

Chapter 6: Resources

Documentation

CMS and CMS Supervisor documents

Title	Description	Audience
Overview		
Avaya Call Management System Overview and Specification	Describes tested product characteristics and product capabilities including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	All user types
Installation, upgrades, maintenance, and troubleshooting		
Deploying Avaya Call Management System	Describes how to install and configure CMS in a virtualized VMware environment.	Implementation engineers, administrators
Deploying Avaya Call Management System in an Infrastructure as a Service Environment	Describes how to deploy CMS in an Amazon Web Services or Google Cloud Platform environment.	Implementation engineers, administrators
Upgrading Avaya Call Management System	Describes the procedures required to upgrade to a new CMS release. This document is focused on full software or platform upgrades.	System administrators, implementation engineers
Maintaining and Troubleshooting Avaya Call Management System	Describes how to configure, maintain, and troubleshoot CMS.	Administrators, support personnel
Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting	Describes how to connect and administer the Automatic Call Distribution (ACD) systems used by CMS.	Administrators, installation personnel, support personnel

Table continues…

Title	Description	Audience
Avaya Call Management System Base Load Upgrade	Describes how to perform a simplified base load upgrade. You can perform a base load upgrade within a CMS release or for other approved scenarios. Not all releases support base load upgrades.	System administrators, implementation engineers
Avaya Call Management System High Availability Connectivity, Upgrade and Administration	Describes how to connect to HA servers and upgrade to HA.	Administrators, installation personnel, software specialists involved with HA
Using Avaya Call Management System High Availability and Admin-Sync	Describes how to install and maintain your CMS High Availability (HA) system.	Administrators, support personnel
Administration		
Administering Avaya Call Management System	Provides instructions on administering a call center using CMS Supervisor.	Avaya support personnel, Administrators
Avaya Call Management System Call History Interface	Describes the format of the Call History data files and how to transfer these files to another computer.	Administrators, supervisors
Using ODBC and JDBC with Avaya Call Management System	Describes how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with CMS.	Administrators, support personnel
Avaya Call Management System Database Items and Calculations	Describes each database item and calculation that CMS tracks and how CMS calculates the values displayed on CMS reports and CMS Supervisor reports.	Administrators, support personnel
Avaya Call Management System Custom Reports	Describes how to design and create custom reports in CMS.	Administrators, report designers
Avaya Call Management System Security	Describes how to implement security features in CMS.	Administrators, support personnel
CMS Supervisor		
Avaya CMS Supervisor Clients Installation and Getting Started	Describes how to install and configure CMS Supervisor.	Implementation engineers, system administrators
Avaya CMS Supervisor Reports	Describes how to use CMS Supervisor reports.	Supervisors, administrators

Table continues…

Title	Description	Audience
Avaya CMS Supervisor Report Designer	Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard.	Supervisors, administrators

Avaya Solutions Platform Documents

Title	Description	Audience
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform server	All user types
Installing the Avaya Solutions Platform 130 Appliance	Describes how to install Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel
Maintaining and Troubleshooting Avaya Solutions Platform 130 Appliance	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel

Finding documents on the Avaya Support website

Procedure

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

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

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

Avaya Documentation Center navigation

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

Important:

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

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

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

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

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** (👁) to add a topic to your watchlist so you are notified when the content is updated or removed.

- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

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

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:

  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

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

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:

  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

  Note:

  Videos are not available for all products.

Support

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

Using the Avaya InSite Knowledge Base

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

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

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

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

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

Appendix A: Blank data forms

Use the forms in this section to record data from the old system. Make copies if you have more than one ACD.

General information

Customer name	
Date	
New CMS model	
New CMS version - Enter: `rpm -qi cms`	
Old CMS name (`uname -n`)	
Old CMS version - Enter: `rpm -qi cms`	

CMS authorizations

Use the `cmssvc` command and select the `auth_display` option. Circle the appropriate authorization or fill in the blanks to note current settings.

Capability/Capacity	Authorization			
forecasting	authorized	not authorized	installed	N/A

Table continues…

Capability/Capacity	Authorization			
external call history	authorized	not authorized	installed	N/A
multi-tenancy	authorized	not authorized	installed	N/A
Dual IP	authorized	not authorized	installed	N/A
Maximum number of split/skill members				
Maximum number of ACDs				
Simultaneous Avaya CMS Supervisor logins				
Number of authorized agents (RTU)				
Number of authorized ODBC connections				
FIPS 140-2				
Firewall				

ACD configuration setup

Use the `cmssvc` command and select the `swinfo` option. Complete for each ACD displayed.

Parameters	ACD 1	ACD 2	ACD 3	ACD 4
Switch name				
Switch model				
Vectoring enabled?				
EAS enabled?				
CO disconnect supervision?				
Phantom abandon timer				
Local port				
Remote port				
Link				
IP address				
TCP port				
Secondary IP address				
Secondary TCP port				

Parameters	ACD 5	ACD 6	ACD 7	ACD 8
Switch name				

Table continues…

Parameters	ACD 5	ACD 6	ACD 7	ACD 8
Switch model				
Vectoring enabled?				
EAS enabled?				
CO disconnect supervision?				
Phantom abandon timer				
Local port				
Remote port				
Link				
IP address				
TCP port				
Secondary IP address				
Secondary TCP port				

Data storage allocation

In CMS, use **System Setup** > **Data Storage Allocation**. Make a copy for each ACD.

ACD Name____					
Data Items	**Number of items**	**Days of intrahour**	**Days of daily**	**Weeks of monthly**	**Months of monthly**
Splits/Skills (0-______)					
Agents					
Trunk groups (0-______)					
Trunks (0-______)					
Call work codes (1-______)					
Vectors (0-______)					
VDNs (0-______)					
Total split or skill members, summed over all splits or skills: ________					

Table continues…

ACD Name________________________________					
Data Items	**Number of items**	**Days of intrahour**	**Days of daily**	**Weeks of monthly**	**Months of monthly**
Number of agent login/logout records: _______					
Number of agent trace records: _______					
Number of unmeasured trunk facilities: _______					
Number of exception records: _______					
Number of call records: _______					

Storage intervals

In CMS, use **System Setup** > **Storage Intervals**. Make a copy for each ACD.

ACD Name____________________________________

Intrahour interval (circle one)

- 15 minutes
- 30 minutes
- 60 minutes

Data summarizing time: __________ AM/PM

Switch time zone offset (-23 to +23): __________

Week start day (circle one)	Sunday	Week stop day (circle one)	Sunday
	Monday		Monday
	Tuesday		Tuesday
	Wednesday		Wednesday
	Thursday		Thursday
	Friday		Friday
	Saturday		Saturday
	Sunday		Sunday

Daily start time: __________ AM/PM

Daily stop time: __________ AM/PM

Backup device

In CMS, use **Maintenance** > **Backup/Restore Devices** to determine your backup device.

Device name: ____________________________________

Path: ____

Description: ____

Device type (circle one)

- 40 GB or larger tape
- USB stick
- NFS mount point

CMS supports upgrades using the following backup devices:

Backup device	Description	Platforms supported
DAT 160	DDS compliant 150 meter 160/ 320-GB DAT cartridge	HPE DL20 G9
DAT 320	DDS compliant 150 meter 320-GB DAT cartridge	HPE DL20 G9
LTO-4	820meter 800-GB 12.65 mm cartridge	HPE DL20 G9
LTO-5	820meter 800-GB 12.65 mm cartridge 846meter 1.5-TB 12.65 mm cartridge	HPE DL20 G9
USB stick	Formatted for Linux, UFS or ZFS, depending on platform	HPE DL20 G9 VMware
NFS mount point		HPE DL20 G9 VMware

No models of 8-mm tape drives are supported. If any backup device other than a supported backup device was administered as the backup device on the old system, a different backup device must be administered on the new system.

Appendix B: Data migration tables

The tables in this section show how CMS handles Informix tables after they are migrated to the new CMS server. Note that the migrated database tables might have been associated with a different backup or restore category in the previous CMS version. For example, a data table that was previously associated with the Agent/Call Center Admin data category might now be associated with the Historical data category.

For data tables in which no category has an X, the data table is reinitialized when CMS is set up on the new system. The data from the old system is not migrated for these tables.

All tables combined

Table[1]	Application	Description	System Admin[1]	Agent/ Call Center Admin[1]	Hist[1]
aar_agents	Agent Act. Recorder	Agents being traced		X	
acd_groups	ACD groups	Global dictionary		X	
acd_shifts	DSA, FSA	Agent shifts		X	
acdadminlog	Historical reports	Log of ACD admin modifications			X
acds	User Permissions	ACD access		X	
ag_actv[2]	Agent Trace	Agent trace data			X
ag_ex_adm	Exceptions	Agent exceptions admin		X	
agex[2]	Historical reports	Agent exceptions data			X
agroups	Dictionary	Agent groups		X	

Table continues…

arch_stat	Archiver	Archive status		X	
arch_tz	Timezone	Timezone administration		X	
br_dev_types	Backup/Restore	B/R device types			
br_devices	Backup/Restore	B/R devices	X		
br_fulls	Backup/Restore	Backup history: full backups			
br_increms	Backup/Restore	Backup history: inc. backups			
br_tables	Backup/Restore	B/R tables			
call_rec	Historical reports	Internal call history			X
cmstbls	Dictionary	Database tables	X		
cow/reports/designer	Supervisor	Report designer	X		
custobjects			X		
customer_log	ELOG	Customer error log			
d_secs	Historical reports				X
dagent[2]	Historical reports	Daily agent data			X
db/gem/c_custom[3]	Custom Reports	Report GEM files (current)	X		
db/gem/h_custom[3]	Custom Reports	Report GEM files (historical)	X		
db/gem/r_custom[3]	Custom Reports	Report GEM files (real-time)	X		
db/journal/shortcut[3]	Time Tables	Shortcut settings	X		
db/journal/timetable[3]	Time Tables	Timetable settings	X		
dberrors	IDBM	Error map: Informix vs. CMS			
dbitems	Dictionary	Database items	X		
dbstatus	Backup/Restore	Hist./forecast tables update status		X	

Table continues…

dcadmin	DSA, SPI, install	Data collection admin			
dcalloc	DSA, FSA	Data storage allocation admin			
dcwc	Historical reports	Daily call work codes data			X
dsplit[2]	Historical reports	Daily splits data			X
dtkgrp[2]	Historical reports	Daily trunk groups data			X
dtrunk	Historical reports	Daily trunks data			X
dvdn	Historical reports	Daily VDNs data			X
dvector	Historical reports	Daily vector data			X
error_msg	ELOG	Canned customer error msgs			
ex_msgs	Exceptions	Canned exception messages			
f_agposrep	Forecast	Agent Positions Required Report			
f_cday[2]	Forecast	Current Day Report			X
f_cdayconf[2]	Forecast	Current Day Config.		X	
f_cdayrep[2]	Forecast	Current Day Report			X
f_chpap	Forecast	Call Handling Profile		X	
f_chprof	Forecast	Call Handling Profile		X	
f_cstap	Forecast	Costs Profile		X	
f_cstprof	Forecast	Costs Profile		X	
f_cstprof	Forecast	Costs Profile		X	
f_dataarch	Forecast	Data Storage Alloc.		X	
f_dsplit2	Forecast	Daily Split Data			X

Table continues…

f_dtkgrp	Forecast	Daily Trunk Group Data			X
f_fin	Forecast	Financial Report			
f_finrep	Forecast	Financial Report			
f_hfinrep	Forecast	Hypothetical Financial Report			
f_hypodata	Forecast	Hypothetical Data	X		
f_hyporep	Forecast	Hypothetical Report			
f_intra	Forecast	Intraday Report			
f_intrarep	Forecast	Intraday Report			
f_ispday[2]	Forecast	Special Day Split Data			X
f_isplit[2]	Forecast	Interval Split Data			X
f_itkgrp	Forecast	Interval Trunk Group Data			X
f_long	Forecast	Long Term Report			
f_longrep	Forecast	Long Term Report			
f_spdays[2]	Forecast	Special Day Admin		X	
f_specrep	Forecast	Special Day Report			
f_status	Forecast	Forecast Manager Status		X	
f_tkgpprof	Forecast	Trunk Group Profiles		X	
f_tkreqrep	Forecast	Trunk Required Report			
f_tperfrep	Forecast	Trunk Performance Report			
features	User Permissions	Feature access	X		

Table continues…

filesys	DSA, FSA	Historical reports file systems			
fs_check	CRT	File systems for free space check			
h_custom[3]	Custom Reports	Custom reports: historical	X		
hagent[2]	Historical reports	Intrahour agent data			X
haglog[2]	Historical reports	Intrahour agent login-logout data			X
hcwc	Historical reports	Intrahour call work code data			X
hsplit[2]	Historical reports	Intrahour split data			X
htkgrp[2]	Historical reports	Intrahour trunk group data			X
htrunk	Historical reports	Intrahour trunk data			X
hvdn	Historical reports	Intrahour VDN data			X
hvector	Historical reports	Intrahour vector data			X
linkex	Historical reports	Link exceptions data			X
m_secs	Historical reports				X
magent[2]	Historical reports	Monthly agent data			X
main_menu[3]	CRT	Main menu	X		
mctex[2]	Historical reports	Malicious call trace exceptions			X
mcwc	Historical reports	Monthly call work code data			X
menu[3]	CRT	Submenu	X		
menu_add[3]	CRT	Menu additions	X		
menu_help	CRT	Menu help			
menu_item_help	CRT	More help for menu items			

Table continues…

msplit[2]	Historical reports	Monthly split data			X
mtkgrp[2]	Historical reports	Monthly trunk group data			X
mtrunk	Historical reports	Monthly trunk data			X
mvdn	Historical reports	Monthly VDN data			X
mvector	Historical reports	Monthly vector data			X
print_adm	Printer Admin	Printer parameters			
r_custom[3]	Custom Reports	Custom reports: real time	X		
scwininfo[3]	Short Cuts	Shortcut window info	X		
sp_ex_adm	Exceptions	Split exceptions admin		X	
spex[2]	Historical reports	Split exceptions			X
split_pro[2]	ACD profiles	Split profile		X	
splits[2]	User Permissions	Split access		X	
std_rpts	Custom Reports	Standard reports list			
synonyms	Dictionary	Synonyms		X	
sys_info	DSA, FSA	DC parameters	X		
ten_agent[4]	Multi-tenancy	Tenant agent assignments		X	
ten_cwc[4]	Multi-tenancy	Tenant Call Work Code assignments		X	
ten_spl[4]	Multi-tenancy	Tenant split/skill assignments		X	
ten_tkgrp[4]	Multi-tenancy	Tenant trunk group assignments		X	
ten_vdn[4]	Multi-tenancy	Tenant VDN assignments		X	
ten_vector[4]	Multi-tenancy	Tenant vector assignments		X	

Table continues…

tenants[4]	Multi-tenancy	Tenant permissions		X	
tg_ex_adm	Exceptions	Trunk group exceptions admin		X	
tgex	Historical reports	Trunk group exceptions			X
tgroups	User Permissions	Trunk groups access		X	
tt_hostname	Time Tables, Host Name	Timetables			
ttsc[3]	Time Tables, User Perms	Timetables	X		
ttsched[3]	Time Tables, User Perms	Schedules	X		
ttsctasks[3]	Time Tables, User Perms	Associated tasks	X		
user_colors[3]	CRT	Color options	X		
user_defval[3]	CRT	User defaults	X		
users[3]	User Permissions	Users	X		
vdn_pro	ACD profiles	VDN profile		X	
vdn_x_adm	Exceptions	VDN exceptions admin		X	
vdnex	Historical reports	VDN exceptions data			X
vdns	User Permissions	VDN access		X	
vec_x_adm	Exceptions	Vector exceptions admin		X	
vecex	Historical reports	Vector exceptions data			X
vectors	User Permissions	Vector access		X	
w_secs	Historical reports				X
wagent[2]	Historical reports	Weekly agent data			X
wcwc	Historical reports	Weekly call work code data			X

Table continues…

workcodes	User Permissions	Work codes access		X	
wsplit[2]	Historical reports	Weekly split data			X
wtkgrp[2]	Historical reports	Weekly trunk group data			X
wtrunk	Historical reports	Weekly trunk data			X
wvdn	Historical reports	Weekly VDN data			X
wvector	Historical reports	Weekly vector data			X

1. Data contained in the tables that are not marked (X) in the System Administration, Agent/ Call Center Administration, or Historical data columns is not migrated to the new system. The tables are empty until the first backup is run.
2. Indicates tables or data affected by the EAS format.
3. Indicates tables that hold data associated with a specific CMS user ID. If the user ID is removed from CMS, an application that uses the migrated data, such as a Timetable report, might report an error and fail.
4. Indicates tables new with CMS R18 that will be migrated when upgrading to future R18 and later releases.You must upgrade a system with Multi-tenancy to a new system that supports Multi-tenancy.

Topic title

Table	Application	Description
br_devices	Backup/Restore	Backup/Restore devices
cmstbls	Dictionary	Database tables
cow/reports/designer	Supervisor	Report designer
custobjects		
db/gem/c_custom[1]	Custom Reports	Report GEM files (current)
db/gem/h_custom[1]	Custom Reports	Report GEM files (historical)
db/gem/r_custom[1]	Custom Reports	Report GEM files (real-time)
db/journal/shortcut[1]	TimeTables	Shortcut settings
db/journal/timetable[1]	TimeTables	Timetable settings
dbitems	Dictionary	Database items
f_hypodata	Forecast	Hypothetical Data

Table continues…

Table	Application	Description
features	User Permissions	Feature access
h_custom[1]	Custom Reports	Custom reports: historical
main_menu[1]	CRT	Main menu
menu[1]	CRT	Submenu
menu_add[1]	CRT	Menu additions
r_custom[1]	Custom Reports	Custom reports: real time
scwininfo[1]	Short Cuts	Shortcut window info
sys_info	DSA, FSA	DC parameters
ttsc[1]	Time Tables, User Perms	Timetables
ttsched[1]	Time Tables, User Perms	Schedules
ttsctasks[1]	Time Tables, User Perms	Associated tasks
user_colors[1]	CRT	Color options
user_defval[1]	CRT	User defaults
users[1]	User Permissions	Users

[1] Indicates tables that hold data associated with a specific CMS user ID. If the user ID is removed from CMS, an application that uses the migrated data, such as a Timetable report, might report an error and fail.

Agent/call center administration tables

Table	Application	Description
aar_agents	Agent Act. Recorder	Agents being traced
acd_groups	ACD groups	Global dictionary
acd_shifts	DSA, FSA	Agent shifts
acds	User Permissions	ACD access
ag_ex_adm	Exceptions	Agent exceptions admin
agroups	Dictionary	Agent groups
arch_stat	Archiver	Archive status
arch_tz	Timezone	Timezone administration
dbstatus	Backup/Restore	Hist./forecast tables update status
f_cdayconf[1]	Forecast	Current Day Config.
f_chpap	Forecast	Call Handling Profile
f_chprof	Forecast	Call Handling Profile
f_cstap	Forecast	Costs Profile

Table continues…

Table	Application	Description
f_cstprof	Forecast	Costs Profile
f_dataarch	Forecast	Data Storage Alloc.
f_spdays[1]	Forecast	Special Day Admin
f_status	Forecast	Forecast Manager Status
f_tkgpprof	Forecast	Trunk Group Profiles
sp_ex_adm	Exceptions	Split exceptions admin
split_pro[1]	ACD profiles	Split profile
splits[1]	User Permissions	Split access
synonyms	Dictionary	Synonyms
ten_agent[2]	Multi-tenancy	Tenant agent assignments
ten_cwc[2]	Multi-tenancy	Tenant Call Work Code assignments
ten_spl[2]	Multi-tenancy	Tenant split/skill assignments
ten_tkgrp[2]	Multi-tenancy	Tenant trunk group assignments
ten_vdn[2]	Multi-tenancy	Tenant VDN assignments
ten_vector[2]	Multi-tenancy	Tenant vector assignments
tenants[2]	Multi-tenancy	Tenant permissions
tg_ex_adm	Exceptions	Trunk group exceptions admin
tgroups	User Permissions	Trunk groups access
vdn_pro	ACD profiles	VDN profile
vdn_x_adm	Exceptions	VDN exceptions admin
vdns	User Permissions	VDN access
vec_x_adm	Exceptions	Vector exceptions admin
vectors	User Permissions	Vector access
workcodes	User Permissions	Work codes access

1. Indicates tables or data affected by the EAS format.
2. Indicates tables new with CMS R18 that will be migrated when upgrading to future R18 and later releases. You must upgrade a system with Multi-tenancy to a new system that supports Multi-tenancy.

Historical tables

Table	Application	Description
acdadminlog	Historical reports	Log of ACD admin modifications

Table continues…

Table	Application	Description
ag_actv[1]	Agent Trace	Agent trace data
agex[1]	Historical reports	Agent exceptions data
call_rec	Historical reports	Internal call history
d_secs	Historical reports	
dagent[1]	Historical reports	Daily agent data
dcwc	Historical reports	Daily call work codes data
dsplit[1]	Historical reports	Daily splits data
dtkgrp[1]	Historical reports	Daily trunk groups data
dtrunk	Historical reports	Daily trunks data
dvdn	Historical reports	Daily VDNs data
dvector	Historical reports	Daily vector data
f_cday[1]	Forecast	Current Day Report
f_cdayrep1	Forecast	Current Day Report
f_dsplit[1]	Forecast	Daily Split Data
f_dtkgrp	Forecast	Daily Trunk Group Data
f_ispday[1]	Forecast	Special Day Split Data
f_isplit[1]	Forecast	Interval Split Data
f_itkgrp	Forecast	Interval Trunk Group Data
hagent[1]	Historical reports	Intrahour agent data
haglog[1]	Historical reports	Intrahour agent login-logout data
hcwc	Historical reports	Intrahour call work code data
hsplit[1]	Historical reports	Intrahour split data
htkgrp[1]	Historical reports	Intrahour trunk group data
htrunk	Historical reports	Intrahour trunk data
fs_check	CRT	File systems for free space check
menu_help	CRT	Menu help
menu_item_help	CRT	More help for menu items
print_adm	Printer Admin	Printer parameters
std_rpts	Custom Reports	Standard reports list
tt_hostname	Time Tables, Host Name	Timetables

[1] Indicates tables or data affected by the EAS format.

Tables not migrated

The data in these tables are not migrated to the new system. The tables are empty until the first backup is run.

Table	Application	Description
br_dev_types	Backup/Restore	Backup/Restore device types
br_fulls	Backup/Restore	Backup history: full backups
br_increms	Backup/Restore	Backup history: incremental backups
br_tables	Backup/Restore	Backup/Restore tables
customer_log	ELOG	Customer error log
dberrors	IDBM	Error map: Informix vs. CMS
dcadmin	DSA, SPI, install	Data collection admin
dcalloc	DSA, FSA	Data storage allocation admin
error_msg	ELOG	Canned customer error msgs
ex_msgs	Exceptions	Canned exception messages
f_agposrep	Forecast	Agent Positions Required Report
f_fin	Forecast	Financial Report
f_finrep	Forecast	Financial Report
f_hfinrep	Forecast	Hypothetical Financial Report
f_hyporep	Forecast	Hypothetical Report
f_intra	Forecast	Intraday Report
f_intrarep	Forecast	Intraday Report
f_long	Forecast	Long Term Report
f_longrep	Forecast	Long Term Report
f_specrep	Forecast	Special Day Report
f_tkreqrep	Forecast	Trunk Required Report
f_tperfrep	Forecast	Trunk Performance Report
filesys	DSA,FSA	Historical reports file systems
fs_check	CRT	File systems for free space check
menu_help	CRT	Menu help
menu_item_help	CRT	More help for menu items
print_adm	Printer Admin	Printer parameters
std_rpts	Custom Reports	Standard reports list
tt_hostname	Time Tables, Host Name	Timetables

Index