CA Chorus™

Installation Guide

Version 03.0.00, Ninth Edition

CA Product References

This document references the following CA Technologies products:

- CA ACF2™ for z/OS (CA ACF2)
- CA Chorus™
- CA Chorus™ for DB2 Database Management
- CA Chorus™ for Security and Compliance Management
- CA Chorus™ for Storage Management
- CA Chorus™ Infrastructure Management for Networks and Systems
- CA Chorus™ Software Manager
- CA Datacom®/AD (CA Datacom/AD)
- CA Distributed Security Interface for z/OS (CA DSI Server)
- CA Detector® for DB2 for z/OS (CA Detector)
- CA Insight™ Database Performance Monitor for DB2 for z/OS (CA Insight)
- CA NetMaster® Network Management for TCP/IP (CA NetMaster NM for TCP/IP)
- CA OPS/MVS® Event Management and Automation (CA OPS/MVS)
- CA RC/Migrator™ for DB2 for z/OS (CA RC/Migrator)
- CA Subsystem Analyzer for DB2 for z/OS (CA Subsystem Analyzer)
- CA SYSVIEW® (CA SYSVIEW)
- CA Top Secret® for z/OS (CA Top Secret)
- CA Vantage™ Storage Resource Manager (CA Vantage SRM)
- Storage Management interface

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Documentation Changes

The following documentation updates have been made since the eighth edition of this documentation:

- Install CA Chorus (see page 21) and Java Home Directory (see page 61)—This release supports IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0 Service Release 2,5 or 7 or IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 1 (5655-W44). Support for Version 7 service release 1 is new.

The following documentation updates have been made since the seventh edition of this documentation:

- How the Installation Process Works (see page 15)—Updated the installation diagram to note the steps that require the use of CA CSM.

The following documentation updates have been made since the sixth edition of this documentation:

- Set TSF Port Assignments Manually (see page 56) and Ports (see page 62)—Noted that you can now set the TSF relay monitor port using the MONPORT parameter in CETJOPTN(TSFRPRMS). (PTFs RO71593 and RO71594 required.)

The following documentation updates have been made since the fifth edition of this documentation:

- How to Load CA Detector Collection Data Automatically (see page 70)—Updated the TSF interval values.
- Install CA Chorus (see page 21) and Java Home Directory (see page 61)—Noted a change in Service Release support. Version 3.0 now supports IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0 **Service Release 2, 5, or 7** (5655-W44), including optional JZOS batch launcher. Support for Service Release 7 is new.
- Install CA Chorus Disciplines (see page 25)—Corrected the low-level qualifier (changed from AE1MJ*type to* AE1M*type)*.
- Configure Your Product Using CA Chorus Software Manager (see page 38)—Added steps to configure the CA Chorus Environment profile.
- Submit CA Chorus and Discipline Jobs (Auto Config) (see page 42)—Added FAWGSMP4 job.

The following documentation updates have been made since the fourth edition of this documentation:

- Install CA Chorus (see page 21)—Added a note to step 6e to alert users that the data set must be able to grow when maintenance is published.

- Multiple Volume Considerations (see page 36)—Added this topic to offer best practices for SMS and non-SMS usage.
- Configure Your Product Automatically (Auto Config) (see page 40)—Added definitions for the key jobs and data sets in this procedure.
- Submit CA Chorus and Discipline Jobs (Auto Config) (see page 42)—Added steps to APF-authorize data sets.
- How to Enable DB2 Object Migration (see page 74)—Removed EXECSTAT from the Object Framework Services (OFS) agent (OFA) configuration, which means that you no longer need to specify the CA Chorus load library (*chorus-hlq*.CETJPLD) in the OFAPROC concatenation.
- JBoss Environment Variables (see page 64)—Added a note to indicate how to add a specific job name for DSI_JOBNAME.
- Use ETJICUST to Point to Another Deployment (see page 59)—Created this standalone topic.

The following documentation updates have been made since the third edition of this documentation:

Legal Notices (see page 2)—Updated to reflect public documentation legal disclaimer.

How the Installation Process Works (see page 15):

- Clarified that you must configure all installed disciplines.
- Clarified in the configuration step that to configure using CA CSM, you must deploy using CA CSM.
- Added reference (step 3) to the Prerequisite Validator.
- Added a stop sign warning to remind you to read the *Site Preparation Guide* before starting the installation.

Installation Methods (see page 18)

- Clarified the new discipline installation method.
- Added "Platform" to the applicable headers.
- Renamed the topic.

Install CA Chorus (see page 21) and Java Home Directory (see page 61)—Noted a change in Service Release support. Version 3.0 now supports IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0 **Service Release 2 or 5** (5655-W44), including optional JZOS batch launcher. Support for Service Release 5 is new.

Install CA Chorus (see page 21) and Install CA Chorus Disciplines (see page 25)—Added a stop sign warning to remind you to read the *Site Preparation Guide* before starting the installation.

Deploying Your Product (see page 29)—Clarified that you must configure all installed disciplines. Deployment is recommended but optional.

Deploy CA Chorus and Disciplines with CA Chorus Software Manager (see page 29)

- Removed erroneous reference to a manual step.
- Clarified the text in the CA CSM registry and remote system steps.
- Added a note to override the path naming standard when editing the custom data set.

Deploy CA Chorus and Disciplines Manually (see page 32)—Simplified the procedure such that two jobs manage the majority of the deployment tasks. (Requires RO63417)

Configuring Your Product (see page 35)—Clarified that you must configure all installed disciplines. Deployment is recommended but optional.

Configuring Your Product Using CA CSM (see page 38)—Clarified the reconfiguration options in step 2.

Submit CA Chorus and Discipline Jobs (Auto Config) (see page 42)

- Clarified in step 1f that you use the *muf_name* that you established when completing prerequisites in the *Site Preparation Guide*.
- Removed an optional CA DSI SSL step that is already covered by the configuration job.
- Simplified the platform steps such that optional steps are now listed last.
- Simplified the introductory text.
- Noted a TSF SUFFIX requirement for upgrades and where to find the commands to make the change.
- Removed an erronenous JBoss configuration job step.
- Noted that you must run E1MI0011/16 or E1MI0012/17 where you installed DB2 or CA Datacom/AD.
- Noted that adding a CA CSM quick link is required.
- Added a note to direct upgrade users to the *Upgrade Guide* to continue.

Seeding Data to Multiple TSF Regions (see page 73)—Removed incorrect reference to TSFSUFFIX default in step 2.

The following documentation updates have been made since the second edition of this documentation:

Configure Your Product Automatically (Auto Config)—Clarified the outcome of step 4. The first paragraph more clearly explains where the new customized data sets reside.

The following documentation updates have been made since the first edition of this documentation:

Installation Use Cases (see page 18)—Clarified the upgrade case.

Deploy CA Chorus and Disciplines Manually—Deleted repetitive mount information from the note in the CA Chorus for Security and Compliance Management steps.

Submit CA Chorus and Discipline Jobs (see page 42)—Updated the CA Chorus for DB2 Database Management job submission information to add an optional step for overriding the DB2 execution mode and to add a warning about starting JBoss during an upgrade.

Verify the Installation and Configuration (see page 48)—Clarified the URL so it includes /Chorus and streamlined the steps to make the URL a trusted site.

Override the DB2 Execution Mode (see page 67)—Added this optional step to the CA Chorus for DB2 Database Management manual configuration tasks.

- Error During Security Discipline Reconfigure Using E1MI0010 or E1MI0020 (see page 58)—Added this troubleshooting topic.
- Error During Security Discipline Reconfigure Using E1MI0014 (see page 58)—Added this troubleshooting topic.

The following documentation updates have been made since the last release of this documentation:

Global—Changed the following references:

- ENV in *chorus_runtime_hlq*.CETJOPTN to ENVETJ.
- Role to discipline
- CA Mainframe Software Manager is now CA Chorus Software Manager
- Changed applicable path references from cetjr2m5 to cetjr3m0.
- Added CA Chorus Version 3.0 FMIDs (CETJ300, CETJ301, and CC2D750)
- Added Third-Party Prerequisite FMID (CETJ302)
- Removed references to CETJZFS1, which does not apply to Version 3.0.
- Changed F2OFAAGT started task name to OFAPROC.
- All platform and discipline installation steps reside in this guide.

Prerequisites and security procedures—Moved this information to the *Site Preparation Guide* because the work must or can be completed prior to the day of the installation.

How the Installation Process Works (see page 15)

- Added a workflow diagram.

- Explained that the installation process begins with work documented in the *Site Preparation Guide.*
- Clarified the deployment and configuration options.

Launch CA Chorus Software Manager—Added this new section.

Installation Use Cases (see page 18)—Added this new section.

Install CA Chorus (see page 21):

- Added CC2D*type* to step 2.
- Changed the AETJHFS reference to AETJZFS.
- Stated more explicitly that you must use PDSE (the default) for a CA Chorus installation.
- Clarified the last two important notes about maintenance.
- Moved the maintenance step to Install CA Chorus Maintenance (see page 27).
- Updated the Java version requirement for 3.0 in step 4.

Install CA Chorus Disciplines (see page 25)—Added this new section.

Install CA Chorus Maintenance (see page 27)—Clarified the steps, listed the FMIDs, and updated the reference information.

Upgrading Your Product—Moved this scenario to a standalone *Upgrade Guide*.

Deploy CA Chorus and Disciplines with CA Chorus Software Manager (see page 29)

- Added information to deploy CA Chorus and each discipline.
- Clarified the requirement to use the file-by-file copy option for custom data sets and added text about deploying platform and discipline at the same time.

Deploy CA Chorus and Disciplines Manually

- Added information to deploy CA Chorus and each discipline.
- Removed references to CETJSIDE, CETJDATV, and CETJZFS1.

Configuring Your Product (see page 35)

- Added explanation for the three configuration options. This topic also indicates where to find the configuration procedures.
- Noted that IPv4 is the default stack. To change it, you must update ENVETJ (see page 63).

Configure Your Product Using CA Chorus Software Manager (see page 38)—Added this new section.

Configure Your Product Automatically—Added this new section.

Post-Installation Considerations (see page 50)—Updated this section for discipline activities.

Verify the Installation and Configuration (see page 48)—Clarified the httpconnectorport definition.

USS Directories (see page 51)—Removed tpv as an option.

Set Port Assignments Manually (see page 54)—Removed ports that apply to Release 2.5 or sooner.

Not Enough Sort Space for CA Datacom/AD—Removed reference to CHDB002, which is no longer valid.

Not Enough Heap Memory—Updated the -Xms and -Xmx values in the workaround steps.

Cannot find a free port JBoss usage—Removed this topic because it does not apply to Version 3.0.

Djboss.remoting.start.portrange—Removed this option because it does not apply to Version 3.0.

CA Chorus Installation Worksheet (see page 61)—Moved this chapter to this guide.

JBoss Environment Variables (ENVETJ) (see page 63) and Ports (see page 62)

- Removed JBoss port for dynamic allocation because it does not apply to Version 3.0.
- Added the -Duser.name and IP stack variable descriptions.
- Added DSIDMPHLQ to JBoss Environment Variables (ENVETJ) (see page 63).
- Clarified that TEIID_MACHINE (see page 63) indicates the CA Chorus machine name.
- Clarified that you need twelve consecutive ports in Ports (see page 62) and JBoss Environment Variables (ENVETJ) (see page 63).

Java Home Directory (see page 61)—Updated the Java version requirement for 3.0.

JAVALIB (see page 61)—Added a description and the default for this installation directory.

Additional CA Chorus for DB2 Database Management Configuration (see page 67)—Added this new section.

Additional CA Chorus for Storage Management Configuration (see page 79)—Added this new section.

Not Enough Sort Space for CA Datacom/AD—Removed this topic because it does not apply to Version 3.0.

JBoss Startup Fails Due to Missing File (see page 53)—Added this new section, which explains how to use the FIXLINK job.

Added the topic to use FIXLINKS in JBoss Startup Fails Due to Missing File (see page 53).

Additional CA Chorus for DB2 Database Management Configuration (see page 67)—Added this new section.

Additional CA Chorus for Storage Management Configuration (see page 79)—Added this new section.

Contents

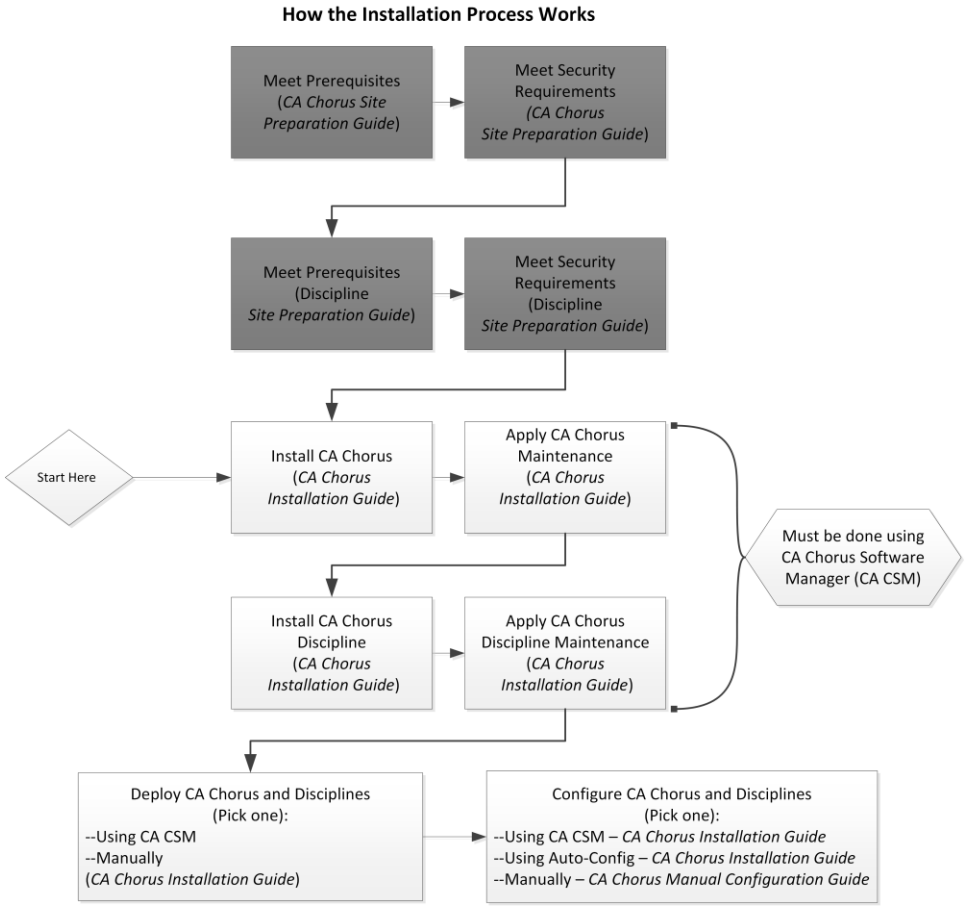
Chapter 1: Installation Process

How the Installation Process Works

The following diagram provides a high-level overview of the CA Chorus and discipline installation, deployment, and configuration process and the guides that you use.

Stop and read the *Site Preparation Guide* before continuing. Do not continue until you have completed all security and prerequisite work as noted in the CA Chorus Platform *Site Preparation Guide* and the applicable discipline *Site Preparation Guide*.

Note: The grayed out boxes indicate tasks that the system administrator and security administrator must have completed before starting the actual installation.



To install, deploy, and configure your CA Chorus and its disciplines, complete the following steps:

Important! Review the following points before you continue:

-- Install the Third-Party Pre-reqs and then the CA Chorus platform before you install any disciplines.
-- You must use CA Chorus Software Manager to install CA Chorus and its disciplines.
-- If you install a discipline, you must deploy and configure it.

1. Meet the software, system, port, and other prerequisites as described in the *CA Chorus Site Preparation Guide*.
2. Meet security requirements as described in the *CA Chorus Site Preparation Guide*.
3. Use the Prerequisite Validator to confirm that you have set up your system correctly as described in the *CA Chorus Site Preparation Guide*.
4. Meet the software, system, port, and other prerequisites as described in the applicable discipline *Site Preparation Guide*. Repeat this step for each discipline that you are installing.
5. Meet security requirements as described in the applicable discipline *Site Preparation Guide*. Repeat this step for each discipline that you are installing.
6. Install CA Chorus and the applicable disciplines using CA Chorus Software Manager as described in the *Installation Guide*. This step involves acquiring the software (transporting to your z/OS system) and installing using SMP/E. The installation process creates a CSI environment and runs the RECEIVE, APPLY, and ACCEPT SMP/E steps. The software is untailored.
7. Deploy CA Chorus and the applicable disciplines using CA CSM or a manual process. The *CA Chorus Installation Guide* details both methods.

   This step copies the target libraries to another system or LPAR.

   Important! For deployments from CA Chorus Software Manager (CA CSM), deploy CA Chorus and your disciplines at the same time. For example, installing CA Chorus, DBA, and Security, and then deploying only CA Chorus and DBA *is not supported*.

   Important! To use the CA CSM Software Configuration Service, CA CSM deployment is required.

8. Configure CA Chorus and the disciplines. This step creates customized load modules, bringing the CA Chorus software to an executable state. You configure the product using one of the following methods:

   Note: We recommend one of the first two options as the most efficient method to configure your products.

   CA CSM

   This method lets you use the wizard-based CA CSM tools to configure the product. For this configuration method, a deployment using CA CSM is required.

   For this method, configure CA Chorus and its disciplines using the *Installation Guide*.

   Automated Configuration

   This method lets you edit one batch job (ETJICUST) and one configuration file. A Java program then propagates your changes to the applicable members. You then manually submit each job. For this option, we recommend that you configure the platform and disciplines at the same time.

   For this method, configure CA Chorus and its disciplines using the *Installation Guide*.

   Manual

   This method lets you manually edit and run each configuration job.

   For this method, configure CA Chorus and its disciplines using the *Manual Configuration Guide*.

   Your CA Chorus system is installed, deployed, and configured.

Installation Methods

Before you begin an installation, review each method. Identify the method that applies to your site and then continue to the next topic for an installation overview.

Important! You must use CA Chorus Software Manager to install CA Chorus and its disciplines.

Important! The CA Chorus platform and each discipline must share the same CSI.

CA Chorus Platform + Discipline Installation

You are installing a new instance of CA Chorus, and you want to install at least one discipline at the same time. Follow the installation instructions and ensure that you install all components into the same CSI name.

New Discipline Installation

You have previously installed the CA Chorus platform, and possibly one or more disciplines, and you now want to install another discipline.

Note the following rules:

- You must use the same CSI as the existing CA Chorus platform (and disciplines, if any). You must redeploy and reconfigure this one CSI as one segment.
  - If you use CA CSM to deploy and configure the discipline using CA CSM SCS, redeploy and reconfigure the platform at the same time using the same CSI.
  - If you use the automatic configuration method, you need only install, deploy, and configure the new discipline.
- After all discipline configuration steps are completed, run ETJI0150 to enable the new discipline, and restart JBoss.

Applying Maintenance to existing CA Chorus Platform and Discipline(s)

You have previously installed the CA Chorus platform, and possibly one or more disciplines, and you now want to apply maintenance to both.

The rules noted in New Discipline Installation apply.

Upgrade CA Chorus with or without a Discipline

The *Upgrade Guide* explains the steps for both scenarios. For the upgrade, you must install a new environment, which means you complete the steps in the *Site Preparation Guides* (platform and discipline) and the *Installation Guide*. You then finalize the configuration and migrate the data based on the steps in the *Upgrade Guide*.

CA Chorus Platform Installation Only - Software Development Kit Implementation

You are installing CA Chorus to use the Software Development Kit (SDK). This list details the high-level tasks to install CA Chorus and view sample SDK data in the Investigator.

Important! As you use the guides to install and configure CA Chorus for SDK-only usage, ignore all discipline steps.

a. Go to the *CA Chorus Site Preparation Guide* and complete all platform tasks.

b. Go to the *CA Chorus Installation Guide*, and complete all platform installation, deployment, and configuration tasks. Do not start JBoss yet or attempt to log in to the product.

c. Go to the *Software Development Kit Guide* and complete *How to Add Your Data and Metadata to the Investigator*.

d. Grant access to this SDK using the user authorization steps in the *CA Chorus Site Preparation Guide*.

e. Start JBoss (CHORJBOS started task) as noted in the *CA Chorus Installation Guide.*

f. Complete the Verify the Installation and Configuration steps as noted in the *CA Chorus Installation Guide*.

Chapter 2: Installing Your Product

Install CA Chorus

Use this process and the CA Chorus Software Manager (CA CSM) documentation to install CA Chorus. After you begin working in CA Chorus Software Manager, a wizard guides you through the steps.

Important! CA Chorus supports only zFS file systems. HFS file systems are not supported.

Note: Use the CA Chorus installation worksheets (see page 61) to record the values that are used at your site for the installation data sets.

Stop and read the *Site Preparation Guide* before continuing. Do not continue until you have completed all security and prerequisite work as noted in the CA Chorus Platform *Site Preparation Guide* and the applicable discipline *Site Preparation Guide*.

Follow these steps:

1. Review Installation Methods (see page 18) to identify which applies to your site.
2. Confirm that you have completed all prerequisite tasks, including running the ETJI095*x* security job, as described in the *Site Preparation Guide*.
3. Log in to CA CSM.
4. Confirm that CA CSM is configured with the system setting to use Product Specific File System. Use the Settings tab to verify this setting. Click Software Installation, scroll to SIS Base Install-File System in the right pane, and verify that the bullet for Product Specific File System is selected.
5. Acquire the product using CA CSM (Products tab) and download the following product installation packages, and any maintenance packages:
   - CA Chorus Third-Party Prerequisites (FMID CETJ302)

     The target libraries consist of USS directories residing under the parent directory /cai/cetjr3m0. The distribution library data set low-level qualifier is TPV.AETJZFS.
   - CA Chorus product (FMID CETJ300, FMID CETJ301, and FMID CC2D750)

     The target libraries are data sets with low-level qualifiers CETJ*type* and CC2D*type*. The USS directory path defaults to /cai/cetjr3m0. The distribution libraries are data sets with low-level qualifiers AETJ*type and* AC2D*type*.

Important! In the following steps, you install the Third-Party Prerequisites first. You then install the CA Chorus product pax file into the CA Chorus Third-Party Prerequisites (JBoss) CSI.

6. Install Third-Party Prerequisites:

   a. Click the Products tab, select the product gen level, locate the CA Chorus Third-Party Prerequisites product package, and select Install.

      If the package was acquired external to CA CSM, complete the following steps:

      - Click Install External Package.
      - Enter the location of the package.
      - Click OK.

   b. Confirm the package data under Introduction, accept the license agreement, and click Next.

   c. Select an installation type.

   d. Click Next at the Prerequisites panel.

e. Create a CSI and set up the global zone, new target zone, and new distribution zone. In most cases, the default values are acceptable; however, update the following parameters:

Note: One of the SMP/E libraries created by this step is the SMPPTS data set, which contains published maintenance. This data set must be able to grow as new maintenance is published. We recommend that this data set be separated from other libraries and allocated on a volume that has sufficient empty space (approximately 2500 cylinders) to avoid E37 abends during the Receive processing.

Important! These values are reused during the CA Chorus configuration, and installation and configuration of the different disciplines. Record the values in a text file using the CA CSM Task ID (see page 24) provided in the Summary Report. Conversely, record them in the CA Chorus installation worksheets (see page 61).

Important! While CA CSM offers a PDS option, you must accept PDSE for SMP/E libraries and user libraries. PDSE is the default.

USS Group Name

Specifies the default USS group (YOURGRP) of the user that is installing CA Chorus. Obtain this value using the **id** command from USS to list the user ID through your security system. For example, the IBM default OMVSGRP is a common value for this field.

HLQ for zFS File Systems

Specifies a high-level qualifier for the CA Chorus zFS file systems. This value can be the same value that is used for the target libraries, the default, or a different high-level qualifier.

Java Home Directory

Specifies the USS directory (without a trailing forward slash) where Java is installed. This directory contains the /bin directory and other files. CA Chorus requires IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0 Service Release 2,5 or 7 (5655-W44) or IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 1 (5655-W44), including optional JZOS batch launcher.

USS Target Directory Name

Specifies the target directory name where CA Chorus is installed. CA CSM mounts a zFS file system in this location so the directory must be a valid USS file system mounting point. If the directory does not exist, it is created. If the directory exists, it must be empty without any file systems mounted to it. If it exists, you are prompted to confirm that it is empty.

For example, /cai/cetjr3m0 is an acceptable value for this field.

f. Review the summary of your selections for the CA Chorus installation, and click Install.

A progress window opens.

If an error occurs during processing, CA CSM prompts you on the Progress tab of the progress window. To review and bypass prompts for certain errors, continue from the Progress tab.

Note: If you are not authorized to mount the existing zFS data set, you are prompted to mount the zFS manually.

Note: If an error occurs during processing, select Show Results and click the failed step to retrieve the generated log files. Conversely, click Download zipped output to download the entire zip file.

A confirmation message indicates that the product is installed. Note the CA CSM task ID for the JBoss installation.

g. (Optional) Click Show Results to review an installation summary.

h. (Optional) Access the CA CSM message log to create a text file of the user parameters that are specified during installation (see page 24).

7. Install the CA Chorus product pax file (CETJ300, CETJ301, and CC2D750 FMIDs) into the CA Chorus Third-Party Prerequisites (JBoss) CSI by following the installation wizard. Note the following points as you use the wizard:

   - Under Prerequisites, select the JBoss SMP/E Environment on the Prereqs panel to indicate the Third-Party CSI that you created previously.
   - Under Target Zone, reuse the target zone parameter values for the CA Chorus JBoss CSI. The USS target directory is filled in with the value specified from the JBoss installation.

Retain User-Specified Parameter Values

Use the CA CSM message log to copy and paste the user parameter values specified during the JBoss installation. This information is necessary for configuration steps later in the installation.

Follow these steps:

1. Note the CA CSM Task ID at the completion of the JBoss installation. This value appears on the installation summary page.
2. Click the Tasks tab, select Task History, and filter by Base Installation.
3. Locate the task ID recorded in Step 1, and select the task for the CA Chorus completed installation.
4. Expand the Preinstallation report, and click the message Log icon.

5. Page forward to the last page of the log to locate the parameter values.
6. Copy and paste the contents of this page into the worksheets (see page 61) that you can reference during the platform and discipline installation and configuration.

   You have collected the user parameter values for reuse during the configuration process.

Install CA Chorus Disciplines

Use this procedure to install each discipline using CA Chorus Software Manager (CA CSM).

Important! Each discipline must be installed into the same CSI and target zone as the JBoss server and CA Chorus.

Stop and read the *Site Preparation Guide* before continuing. Do not continue until you have completed all security and prerequisite work as noted in the CA Chorus Platform *Site Preparation Guide* and the applicable discipline *Site Preparation Guide*.

Follow these steps:

1. Review Installation Methods (see page 18) to identify which applies to your site.
2. Acquire each discipline by downloading the product package from the Software Catalog tab:

   Note: Each FMID includes everything that is required for each discipline component.

   - **CA Chorus for DB2 Database Management**:
     - This package includes the CE3K*nnn* FMID (*nnn* identifies the version and release).
     - The target libraries are data sets with low-level qualifiers CE3K*type*. The USS directory path defaults to /cai/cetjr3m0/roles/dba on CE3KZFS.
     - The distribution libraries are data sets with low-level qualifiers AE3K*type*.
   - **CA Chorus Infrastructure Management for Networks and Systems**:
     - The package includes the CFAW*nnn* FMID (*nnn* identifies the version and release).
     - The target libraries are data sets with low-level qualifiers of CFAW*type*. The USS directory default mount point is /cai/cetjr3m0/roles/performance for the file system name with the low-level qualifier of CFAWZFS.
     - The distribution libraries are data sets with low-level qualifiers AFAW*type*.
   - **CA Chorus for Security and Compliance Management**:
     - This package includes the CE1M*nnn* FMID (*nnn* identifies the version and release).
     - The target libraries are data sets with low-level qualifiers CE1Mtype. The USS directory default mount point is /cai/cetjr3m0/roles/security on CE1MZFS.
     - The distribution libraries are data sets with low-level qualifiers AE1M*type*.
   - **CA Chorus for Storage Management**:
     - This package includes the CE4H*nnn* FMID (*nnn* identifies the version and release).

- The target libraries are data sets that start with low-level qualifiers CE4H*type*. The USS directory default mount point is /cai/cetjr3m0/roles/storage for the file system name with the low-level qualifier of CE4HZFS.
- The distribution libraries are data sets that start with low-level qualifiers AE4H*type*.

3. Install each discipline:
   a. Click the Products tab, select the product gen level, locate the discipline package as noted in Step 1, and select Install.

      Note: If the package was acquired external to CA CSM, click Install External Packages, enter the location of the package, and click OK.

   b. Confirm the package data under Introduction, accept the license agreement, and click Next.

   c. Select an installation type.

   d. Under Prerequisites, select the CA Chorus SMP/E Environment on the Prerequisites panel to indicate the CA Chorus CSI that you created previously.

   e. Under the CA Chorus TARGET zone, reuse the target zone parameter values for the CA Chorus CSI. The USS target directory is filled in with the value specified from the JBoss installation.

   f. Review the summary of your selections for the CA Chorus installation, and click Install.

      A progress window opens. This process can take several minutes to complete. Monitor the progress of the installation by clicking the Progress tab.

      Note: If an error occurs during processing, take one of the following actions:

      - Click the step that failed to retrieve the generated log files.
      - Click Download zipped output.

      A confirmation message indicates that discipline is SMP/E installed successfully.

   g. (Optional) Click Show Results to review an installation summary.

Install CA Chorus and Discipline Maintenance

After you install CA Chorus and its disciplines, use the following process to apply maintenance to CA Chorus (all FMIDs) and the applicable disciplines through CA Chorus Software Manager.

If you have deployed and configured CA Chorus, the maintenance is applied to your SMP/E target data sets.

Follow these steps:

1. Review Installation Use Cases (see page 18) to identify which applies to your site.
2. Click the SMP/E Environments tab.
3. Click Refresh in the upper-right corner.
4. Select the CA Chorus or discipline CSI link, and click Maintenance.
5. Select All in your filter, or select only the PTFs that you need.
6. Click Install to install the PTFs.
7. Follow the wizard prompts to complete the installation.

   The PTFs are installed and maintenance is applied.
8. Click Refresh to confirm the status of the PTF installation.

   Maintenance is applied.

   Important!

   For CA CSM: If you are using the deployment and configuration services, to finalize the application of maintenance, redeploy and reconfigure the platform and all disciplines in your CSI.

   For Automatic Configuration: If you have deployed and configured your product, the maintenance is applied to your SMP/E target data sets. To deploy the maintenance to your deployed and configured data sets, copy only the data sets that are affected by the maintenance to your deployed data sets. If the maintenance applies to a zFS file system, rerun ETJI0100 in *chorus__runtime_hlq*.CETJJCL to ensure that the correct USS permissions are set. In general, any fix that affects the following data sets can affect completed customizations:

   CETJEZTR CETJJCL

   CETJOPTN CETJOPTV

   CETJPROC CE1MJCL

   CE1MOPTV CE3KJCL

   CE3KPARM CE4HJCL

   CFAWJCL

   This type of fix contains appropriate information in the HOLDDATA. In general, any fix that affects your discipline FMID can affect completed customizations.

Chapter 3: Deploying Your Product

Important! To use the CA Chorus Software Manager (CA CSM) Software Configuration Service (SCS), CA CSM deployment is required.

Important! If you install a discipline, you must deploy and configure it.

Important! When you execute a deployment manually or using CA CSM, previously configured libraries could be overlaid with user edits being lost. Therefore, we recommend that you create a custom CA Chorus Platform where copies of the edited members can reside. Doing so protects you from losing the edits. This issue does not apply when you use auto-configuration. If you use SCS, configuration metadata customizations are reapplied to create updated, customized libraries. Any user modification to the files created by SCS are lost. You must reapply manual edits to the files customized by SCS.

To proceed, go to the CA CSM Deployment procedure or the manual deployment procedure.

Deploy CA Chorus and Disciplines with CA Chorus Software Manager

Deployment lets you take your installed software and copy it onto systems across your enterprise. The software can then be configured for use on those systems. The deployed objects include target libraries that are defined to SMP/E and user-selected data sets.

Important! For deployments from CA Chorus Software Manager (CA CSM), deploy CA Chorus and your disciplines at the same time. For example, installing CA Chorus, Storage and Security, and then deploying only CA Chorus and Storage is not supported.

Follow these steps:

1. Allocate new data sets on the deployment target system:

   Note: The first two steps deploy JBoss and CA Chorus in a single deployment operation of the two deployable units. Verify that the installation zFS data sets are still mounted. If needed, remount manually before the deployment.

   a. Copy DPLSAMP1 and DPLSAMP2 from *your_chorus_hlq.*CETJJCL to the deployment target system.

      Repeat this step for each discipline:

      - **For CA Chorus for DB2 Database Management**: E3KDSMP1 and E3KDSMP2 from *your_chorusdba_hlq.*CE3KJCL
      - **For CA Chorus Infrastructure Management for Networks and Systems**: FAWDSMP1 and FAWDSMP2 from *your_chorusperf_hlq.*CFAWJCL
      - **For CA Chorus for Security and Compliance Management**: E1MDSMP1 and E1MDSMP2 from *your_chorussec_hlq.*CE1MJCL
      - **For CA Chorus for Storage Management**: E4HDSMP1 and E4HDSMP2 from *your_chorusstor_hlq.*CE4HJCL

   b. Edit and submit DPLSAMP1 and DPLSAMP2 on the deployment target system to allocate and mount the CA Chorus zFS data set CETJZFS0 for that deployed instance.

      Repeat this step for each discipline. Use the members and data sets noted in step 1a.

      Note: The USS path that is associated with the zFS file system is automatically added as a custom data set when the product is added to the Deployment definition.

      Note: We recommend that the zFS file systems be permanently mounted by including them in the SYS1.PARMLIB(BPXPRM*xx*) member.

2. Set up the CA CSM system registry. Complete the following steps from the System Registry tab:

   a. Determine the systems that you have at your enterprise.

   b. Set up the target systems and validate them.

   c. Add network information, including data destination information, to each system registry entry.

3. Set up remote credentials for the systems addressed in the previous step. Do so from the Settings tab.

4. Set up methodologies that determine what to allocate on the target system. Do so from the Deployments tab.

5. Start the deployment by completing each step in the New Deployment wizard:

   a. Create the deployment, but do not perform the actual deployment.

      The deployment can be changed later by adding and editing systems, products, customer data sets, and methodologies, or you can deploy directly from the wizard.

      Note: Create a separate deployment to deploy other products to the previously defined systems using the same methodologies.

   b. Edit the custom data set (CETJZFS0) in the deployment.

      Note: When you are editing the data, click Check Override Path Naming standard.

      Repeat for each discipline:

      Note: If you change the paths in the following bullets, specify the name as specified in the discipline SAMP job.

      - **For CA Chorus for DB2 Database Management**: CE3KZFS. The local path defaults to /cai/cetjr3m0/roles/dba. If you enter /cai/dply/cetjr3m0/roles for the remote path, CA CSM creates the following path on the remote system: /cai/dply/cetjr3m0/roles/dba.
      - **For CA Chorus Infrastructure Management for Networks and Systems**: CFAWZFS. The local path defaults to /cai/cetjr3m0/roles/performance. If you type /cai/dply/cetjr3m0/roles for the remote path, CA CSM creates the following path on the remote system: /cai/dply/cetjr3m0/roles/performance.
      - **For CA Chorus for Security and Compliance Management**: CE1MZFS. The local path defaults to /cai/cetjr3m0/roles/security. If you enter /cai/dply/cetjr3m0/roles for the remote path, CA CSM creates the following path on the remote system: /cai/dply/cetjr3m0/roles/security.
      - **For CA Chorus for Storage Management**: CE4HZFS. The local path defaults to /cai/cetjr3m0/roles/storage. If you type /cai/dply/cetjr3m0/roles for the remote path, CA CSM creates the following path on the remote system: /cai/dply/cetjr3m0/roles/storage.

      Important! For custom data sets, use the file-by-file copy option and enter the path of the remote directory as specified in the customized sample deployment jobs.

   c. Save the deployment.

6. Deploy the product. This process takes a snapshot, copies it to the target system, and deploys (unpacks) on the target.

   The product is now ready to configure. Go to Configuring Your Product (see page 35).

Deploy CA Chorus and Disciplines Manually

Use this procedure to deploy CA Chorus and its disciplines manually. The steps include subheadings to identify where the steps begin for each discipline.

This procedure requires that you have applied RO63417.

Important! You must deploy all installed disciplines.

Follow these steps:

1. Copy the PACKAGE job from *your_chorus_hlq*.CETJJCL to an alternate library.

   Important! If you submit the PACKAGE from within the target library which we are attempting to dump, the job can fail due to contention.

2. Execute the PACKAGE job on the LPAR where CA Chorus and your disciplines are installed.

   All CA Chorus installation data sets, irrespective of the DS organization (PS/PDS/PDSE/VSAM,) are dumped into a sequential data set.

3. (Optional) If you are deploying to a remote LPAR, FTP the dump data set (CAI_INSTALL_HLQ.PACKAGE) and the DEPLOY member that is delivered in the installation library *your_chorus_hlq*.CETJJCL to a data set on the remote LPAR so it can be configured and run. Ensure that you have allocated a PACKAGE data set on the remote LPAR such that FTP does not result in B37 abends.

4. Execute the DEPLOY job from *your_chorus_hlq*.CETJJCL on a local or remote LPAR.

   The deployment is complete.

5. Remount the zFS file systems as needed after the data sets are successfully copied.

   Important! If you are using CA Chorus only for the SDK, you are ready to configure the product.

   Note: Mount CETJZFS0 R/W at the target or remote CA Chorus home directory. Review, modify, and submit DPLSAMP2 in CETJJCL to mount the zFS data sets. This job only mounts the Install Home zFS for you. Doing so can help you avoid a manual mount.

   CA Chorus Infrastructure Management for Networks and Systems Deployment Steps

6. Remount the zFS file systems as needed after the data sets are successfully copied.

   CA Chorus Infrastructure Management for Networks and Systems is now ready for you to configure.

   Note: Mount CFAWZFS R/W at the /roles/performance directory (inside CETJZFS0). Review, modify, and submit FAWDSMP2 in *your_chorusperf_hlq*.CFAWJCL to mount this discipline's zFS data sets.

CA Chorus for Security and Compliance Management Deployment Steps

7. Remount the zFS file systems as needed after the data sets are successfully copied.

   CA Chorus for Security and Compliance Management is now ready for you to configure.

   Note: Mount CE1MZFS R/W at the /roles/security directory (inside CETJZFS0). Review, modify, and submit E1MDSMP2 in *your_chorussec_hlq.*CE1MJCL to mount this discipline's data sets.

CA Chorus for Storage Management Deployment Steps

8. Remount the zFS file systems as needed after the data sets are successfully copied.

   CA Chorus for Storage Management is now ready for you to configure.

   Note: Mount CE4HZFS R/W at the /roles/storage directory (inside CETJZFS0). Review, modify, and submit E4HDSMP2 in *your_chorusstor_hlq*.CE4HJCL to mount this discipline's zFS data sets.

Chapter 4: Configuring Your Product

Choose one of the following configuration methods:

Important! We recommend the first two options as the most efficient methods to configure your products. Before you start configuring your product, review Multiple Volume Considerations (see page 36).

CA Chorus Software Manager (see page 38)

You use this wizard-based tool to configure the product. To use the CA CSM Software Configuration Service, CA CSM deployment is required.

Automated Configuration

You edit one batch job (ETJICUST) and one configuration file. A Java program then propagates your changes to the applicable members. You then manually submit each job. For this method, we recommend that you configure the platform and disciplines at the same time.

Important! If you are using this method, we recommend that you first install and deploy the platform *and* disciplines.

Manual

You manually edit and run each job in the configuration sequence. For this method, see the *Manual Configuration Guide* for platform and discipline procedures.

Multiple Volume Considerations

Multiple volume allocations are required when a data set allocation is expected to consume more space than, which is available on a single volume. Review this topic to understand how to enable multiple volume/extent support when using non-SMS- or SMS-managed allocations.

SMS automatically manages storage-space related issues. However, you may encounter situations where SMS is not an option. Adequately addressing your storage needs before configuration can ensure that you complete the procedure without SB37/SD37/SE37 abends.

Important! This topic applies to Automatic Configuration users. CA CSM does not support multiple volume designations.

Non-SMS usage

If the space is insufficient on a data set allocation, request more volume serials. For example, code VOLUME=SER=(ser1,ser2,ser3) to request three volume serials on the specified device.

Use non-SMS for the following cases:

- SMS is not used at all.
- To direct a particular data set to a particular volume.

SMS Extents

If the space is insufficient on a data set allocation, request more units. For example, replace UNIT=3390 with UNIT=(3390,2) to request two units on specified STORCLAS.

Example Use Cases

You have installed and deployed CA Chorus. Before you configure the product, you want to understand how to configure multiple volumes using non-SMS and/or multiple SMS extents. In both cases, you are increasing the volumes to help with a database backup.

Auto Configuration sample: Non-SMS

If you are using non-SMS and to allocate a large format dataset to three multiple volumes, replace it with VOL=SER=(DASD01,DASD02,DASD03). In the following sample, the bold text indicates the change location within the Auto Configuration CONFIG.DATA file.

```
//*RT_UNIT - DASD storage UNIT type for new datasets
//* Special characters must be enclosed in apostrophes.
//* If you are using SMS values for the SET RT_DD_STORAGE keyword,
//* leave this value as the default (3390).
//* DFSMS overrides the UNIT keyword automatically with the UNIT
//* that the SMS volume needs.
// SET RT_UNIT='UNIT=3390'
//*SET RT_UNIT='UNIT=(3390,n)'
//*
//*RT_VOLUME - DASD volume for non-SMS allocations
// SET RT_VOLUME='VOLUME'
//*SET
RT_VOLUME='(VOLUME1,VOLUME2,VOLUME3)'

//*
//*RT_VOLSER - DASD VOL=SER number for new datasets: non-SMS allocations
//* Note:
//* a. Special characters must be enclosed in apostrophes.
//* b. For SMS allocations, this symbol can be left as-is.
// SET RT_VOLSER='VOL=SER=@RT_VOLUME@'
```

Auto Configuration sample: SMS Extents

In the following sample, the bold text indicates the change location within the Auto Configuration CONFIG.DATA file to use SMS extents.

```
//*RT_UNIT - DASD storage UNIT type for new datasets
//* Special characters must be enclosed in apostrophes.
//* If you are using SMS values for the SET RT_DD_STORAGE keyword,
//* leave this value as the default (3390).
//* DFSMS overrides the UNIT keyword automatically with the UNIT
//* that the SMS volume needs.
// SET RT_UNIT='UNIT=3390'
//*SET RT_UNIT='UNIT=(3390,n)'
//*
//*RT_VOLUME - DASD volume for non-SMS allocations
// SET RT_VOLUME='VOLUME'
//*
//*RT_VOLSER - DASD VOL=SER number for new datasets: non-SMS allocations
//* Note:
//* a. Special characters must be enclosed in apostrophes.
//* b. For SMS allocations, this symbol can be left as-is.
// SET RT_VOLSER='VOL=SER=@RT_VOLUME@'
```

Important! After you run ETJICUST more than once, the runtime JCL appears as follows to enable SMS multiextent allocation for data sets:

```
//BKP4003B DD DSN=CAI.CHORUS.DATACOM.TSF4003.NEW,
//            DISP=(NEW,CATLG,DELETE),
//            STORCLAS=SCTSO,
//            MGMTCLAS=MCTSO,
//            UNIT=(3390,3),DSNTYPE=LARGE,
//            SPACE=(CYL,(2000,500),RLSE
```

Configure Your Product Using CA Chorus Software Manager

Configuration copies the deployed libraries to run-time libraries and customizes the product for your site to bring it to an executable state. You can configure CA Technologies products that you have already acquired, installed, and deployed using CA Chorus Software Manager (CA CSM). You cannot use CA CSM to configure a product unless you have already used CA CSM to deploy the product.

Important! If you install a discipline, you must deploy and configure it.

Use this outline and the CA CSM online help to configure CA Chorus and its disciplines:

1. Select a configurable deployment on the Deployments tab to view details and products for that deployment.
2. Determine your installation type and the steps to take based on the following points:
   - For a new installation, create a CA Chorus configuration as described in the next step.
   - If you are applying maintenance or adding a discipline to a CA Chorus Platform, you can select the reconfigure option in CA CSM.
     - A reconfiguration lets you preserve existing user data. If you reconfigure a CA Chorus Platform, you must also reconfigure associated discipline instances.
     - If you reconfigure, you must delete the existing configuration definition. Deleting this definition does not delete the data sets. The operations associated with the reconfigure will delete and recreate the data sets containing the updated software, but will retain the data sets containing user data.

   You have identified your installation type. Go to the next step.
3. Select the CA Chorus Platform in the deployment and start the Configuration wizard to create a configuration. Complete each of the steps in the wizard. The wizard has multiple levels of detailed instructions and guides you through choosing configuration settings for your site. At any point, you can save your work and return to it later. Configurations where you have partially completed the steps in the wizard are listed on the Configurations tab.

   Note: For some configurations, you must edit resources. Edit instructions appear above the resource in the editor.

   a. Define a configuration name and select a target system.

   b. Select configuration functions and options.

   c. Define system preferences.

   d. Create target settings.

   e. Select and edit resources.

   f. Review the build.
4. Build the configuration. The last step of the Configuration wizard lets you build the configuration. If needed, you can edit the configuration and can build the configuration again. Building the configuration closes the wizard and creates a configuration with all of your settings.
5. Locate your configuration in the Configuration tab.
6. Validate the configuration. Validation verifies access to resources that are going to be used when you implement the configuration.

7. Implement the configuration. You implement a configuration to make your deployed software fully functional. Implementation executes on the target system, applying the variables, resources, and operations that are defined in the configuration.

   CA CSM configures the product.

8. Complete the tasks in Verify the Installation and Configuration (see page 48) and Post Installation Considerations (see page 50).

   CA Chorus and the applicable disciplines are configured.

9. Update the CA Chorus Environment profile before you attempt to configure any disciplines. To do so, go to the Systems Registry tab.

10. After clicking the Create Occurrence for this Environment profile, provide a suitable name for PLATFORM_NAME (for example, CA_CHORUS_V3.0), and click Save. Locate this occurrence on the System Registry and provide values as used during the Platform Configuration. The VERSION should be 03000.

    Note: While doing Platform Reconfiguration or Discipline Configuration, you will be presented with the Define System Preferences panel to select this occurrence.

    CA Chorus is configured and ready for use.

11. Repeat this procedure for each discipline. Use the system registry that you created for the CA Chorus Platform.

Configure Your Product Automatically (Auto Config)

The automated configuration simplifies the configuration process. We recommend that you configure CA Chorus and disciplines at the same time.

Important! In *your_chorus_hlq*.CETJJCL and other data sets, you see seemingly duplicate members. For example, CHORJBOS and $HORJBOS. The first member is for manual configuration use. The second member is for automatic configuration use; however, with this method, you do not manually update any members that lead with the $ symbol. The ETJICUST batch job updates these members for you.

Important! If you install a discipline, you must deploy and configure it.

Follow these steps:

Important! Read the JCL comments as you complete this procedure. Most procedural and reference details reside in the jobs.

1. Review the following auto-config terms:

   ETJICUST

   A customization job that lets you propagate site-specific variables from one data set to all members of the library under your HLQ. You run this job twice in this procedure.

   - **First Run**: Creates your configuration data set, which contains all variables needed for your configuration. At this point, these variables have sample/default values. In subsequent steps, you will edit them to provide site-specific values.You only see variables for the disciplines that you are installing/configuring.
   - **Second Run**: In this run, your configuration data sets serves as the input to customize the members in the libraries with the HLQ provided in Output_ds_HLQ. These are new libraries that are created in this run of ETJICUST.

   Configuration Data Set (Configuration_ds)

   This data set includes directions and definitions regarding the values that you must enter for the CA Chorus and discipline configuration. You specify and create this data set during the first run of ETJICUST.

   Output_ds_HLQ

   Your configuration settings are applied to the CA Chorus and discipline configuration members in the new customized data sets as specified under the Output_ds_HLQ variable in the ETJICUST JCL member.

2. Review and edit ETJICUST in *your_chorus_hlq*.CETJJCL.
3. Submit ETJICUST in *your_chorus_hlq*.CETJJCL.

   Note: (*New configurations only*) For the configuration data set that you specify in the first run of this job, you cannot specify a data set that already exists.

   The expected return code is zero. Your configuration data set is created.

4. Edit the configuration data file that you specified for Configuration_ds as defined in ETJICUST. This data set includes directions and definitions regarding the values that you must enter for the CA Chorus and discipline configuration. Some values are optional, and some are mandatory.
5. Resubmit ETJICUST in *your_chorus_hlq*.CETJJCL.

   The expected return code is zero. If you see a different return code, review the output, make the appropriate change, and rerun the job.

Your configuration settings are applied to the CA Chorus and discipline configuration members in the new customized data sets as specified under the Output_ds_HLQ variable in the ETJICUST JCL member. In the following topic, you submit the preconfigured jobs from these data sets.

Important! You may determine that you have entered an incorrect value in the Configuration_ds file (for example, you see a customized job with incorrect information). For this scenario, update the information in the Configuration_ds file, and rerun ETJICUST. Doing so reconfigures the customization jobs and ensures that all values are updated correctly.

More information

Use ETJICUST to Point to Another Deployment (see page 59)

Submit CA Chorus and Discipline Jobs (Auto Config)

Use this procedure to submit the jobs that the automated configuration process edited. In the following steps, use the jobs that include *custom* in the high-level qualifier (HLQ).

Important! If your site does not include a discipline, skip the step. Additionally, if you are installing CA Chorus to use only the Software Development Kit, skip all discipline steps.

In the following procedure, you mount and APF-authorize several data sets. Within the procedure, these actions are temporary. You can make them permanent by moving them to PARMLIB as noted in Post Installation Considerations (see page 50).

Follow these steps:

Note: For each of the following steps, review the output to confirm that your submissions succeeded. If a submission fails, use the return code to resolve any issues.

CA Chorus Job Submission

1. Submit the following CA Chorus jobs:
   a. ETJI0100 from *custom_hlq*.CETJJCL (Changes zFS ownership)
   b. ETJI0101 member from *custom_hlq*.CETJJCL (Mounts user file systems)
   c. ETJUDCDF and ETJUDCMT from *custom_hlq*.CETJJCL (Configures the Knowledge Center zFS)
   d. APF-authorize the following data sets:
      - *custom_hlq*.CC2DLOAD (Includes the Time Series Facility (TSF) library)
      - *custom_hlq*.CETJLOAD (Includes the CA Chorus library)
      - *custom_hlq*.CETJPLD (Includes the CA Chorus library)

      Choose *one* of the following options to complete the APF-authorization step:

      - If you are using CA SYSVIEW, submit ETJAPFAD from *custom_hlq*.CETJJCL.
      - If you are not using CA SYSVIEW, enter the following commands:

      ```
      SETPROG APF,ADD,DSNAME=custom_hlq.CC2DLOAD,<SMS|volume=volume>
      SETPROG APF,ADD,DSNAME=custom_hlq.CETJPLD,<SMS|volume=volume>
      SETPROG APF,ADD,DSNAME=custom_hlq.CETJLOAD,<SMS|volume=volume>
      ```

      volume

      Defines the volume label for the name of the disk. If you are using SMS, do not define a *volume*.

      Note: As part of the CA Datacom/AD prerequisite, the following libraries should also be APF-authorized: *datacomad_adthlq*.CAAXLOAD (CA Datacom/AD load library) and *datacomad_adchlq*.CUSLIB (CA Datacom/AD customization library).
   e. CPYAXDAT from *custom_hlq*.CETJJCL to copy AXDATIN1 and AXDATIN2 settings from CETJOPTN to &ADCHLQ.CUSMAC.
   f. Start the CA Datacom/AD MUF for CA Chorus (/S *your_muf_name*). You established the name of this MUF during the prerequisite setup as noted in the software requirements of the *Site Preparation Guide*.
   g. CHDB004 from *custom_hlq*.CETJJCL (Initializes the tables and defines the data sources)

      Note: To clean up and restart the initialization, execute the CHDB101 member in *custom_hlq*.CETJJCL, execute the CHDB102 member in *custom_hlq*.CETJJCL, and repeat 1g.
   h. TSDB002 from *custom_hlq*.CETJJCL (Allocates and defines the TSF database to the CA Datacom/AD MUF)

Note: If a step fails, the remaining steps do not execute. To clean up and restart the initialization, execute the TSDB102 member in *custom_hlq*.CETJJCL, execute the CHTSDBDL member in *custom_hlq*.CETJJCL, and repeat step 1h.

Important! The TSF metric database uses large amounts of disk space. We strongly recommend that you set up automation to reclaim free space and monitor your database space usage. For information about setting up this automation, see the *Administration Guide*.

i. TSF#ALOC from *custom_hlq*.CETJJCL (Allocates the TSF VSAM data sets)

j. TSF#PPL8 from *custom_hlq*.CETJJCL (Populates the TSF VSAM data sets)

k. Copy customized CHORTSF from CETJJCL to PROCLIB

Note: A suffix serves as the ID for TSF engines. If you are completing this procedure for an upgrade and if you have multiple CHORTSF instances on the same LPAR, you must change the suffix. To do so, see Add the Time Series Facility Settings in the *Upgrade Guide*.

l. Start TSF (/S CHORTSF).

Note: As part of the startup process, this job dynamically determines the associated ports (such as TSF query).

m. ETJI0145 from *custom_hlq*.CETJJCL. (Configures the JDBC driver for CA Datacom/AD)

n. ETJI0140 from *custom_hlq*.CETJJCL (Adds a CA Chorus Software Manager link to the Quick Links module) If you are using an APPL name that differs from the default value for CA CSM (CSMAPPLM), modify the msmApplid in ENVETJ of *custom_hlq*.CETJOPTN.

o. (Optional) ETJI0110 member in *custom_hlq*.CETJJCL (Enables or disables HTTPS)

p. (Optional) If your TSF configuration includes a remote system, copy the customized CHORTSFR to a remote system PROCLIB and then start the CHORTSFR (/S CHORTSFR).

q. (Optional) If you are using an SMTP server to send notification emails for crossed policy thresholds, submit ETJI0135 from *custom_hlq*.CETJJCL.

r. (Optional) To set up High Availability, see the *Administration Guide* to review all HA implications, and then submit ETJARMP from *custom_hlq*.CETJJCL.

Important! Steps 2 through 5 detail the jobs to submit for each discipline. Complete the applicable steps and then go to step 6.

CA Chorus for DB2 Database Management Job Submission

2. Submit the following CA Chorus for DB2 Database Management jobs:

   Important! Before finalizing DB2 subsystem connections in the following step, see the *Manual Configuration Guide* for a detailed explanation of DBA subsystems, confederations, and data sources.

   a. E3KI0010 in *custom_hlq*.CE3KJCL (Defines DB2 subsystem connections)

   b. E3KI0020 in *custom_hlq*.CE3KJCL (Defines data sources). The MUF must be active when you submit this job.

      Note: To clean up and restart the initialization, submit the CHDB101 member in *custom_hlq*.CETJJCL, CHDB102 member in *custom_hlq*.CETJJCL, CHDB004 from *custom_hlq*.CETJJCL, and repeat step 2b.

      Important! The next three substeps must be performed manually.

   c. (Optional) If you are running any DB2 subsystems in Compatibility Mode (CM), override the DB2 execution mode (edit E3KMOD10 in *your_chorusdba_hlq*.CE3KPARM, and edit and submit E3K3I0030 in *your_chorusdba_hlq*.CE3KJCL).

      Note: The configuration tasks in the next two substeps are not required for an integration with CA Chorus Infrastructure Management for Networks and Systems.

   d. Load CA Detector collection data for the TSF. Complete the tasks under Statistics Gathering Overview (see page 69).

   e. Enable DB2 object migration. Complete the steps in How to Enable DB2 Object Migration.

      Note: When you complete substeps c and d, return to this topic to complete the configuration.

CA Chorus Infrastructure Management for Networks and Systems Job Submission

3. Submit each of the following CA Chorus Infrastructure Management for Networks and Systems jobs:

   a. FAWGSMP1 from *custom_hlq*.CFAWJCL (Sets the CA NetMaster NM for TCP/IP properties)

   b. FAWGSMP2 from *custom_hlq*.CFAWJCL (Sets the CA SYSVIEW properties)

   c. FAWGSMP3 from *custom_hlq*.CFAWJCL (Configures the sysview-module.xml file)

   d. FAWGSMP4 from custom_hlq.CFAWJCL (Re-establish hard links and symbolic links for USS run-time environment).

CA Chorus for Security and Compliance Management Job Submission

4. Submit the following CA Chorus for Security and Compliance Management jobs:

   a. E1MI0010 member in *custom_hlq.*CE1MJCL (Establishes database connections)

   b. E1MI0020 member in *custom_hlq*.CE1MJCL (Creates the CA LDAP files)

      Note: For the next two steps, run these jobs where DB2 or CA Datacom/AD is installed.

   c. E1MI0011 (DB2) or E1MI0016 (CA Datacom/AD) in *custom_hlq*.CE1MJCL (Creates CIA database views)

   d. E1MI0012 (DB2) or E1MI0017 (CA Datacom/AD) in *custom_hlq*.CE1MJCL (Creates CA Compliance Manager database views)

   e. E1MI0014 member in *custom_hlq.*CE1MJCL (Defines the Security and Policy Administration nodes)

   f. E1MI0015 in *custom_hlq.*CE1MJCL (Identifies the systems for use with the Security Command Manager module)

   g. If you have CA DSI Servers running systems that are configured for use with the Security Command Manager module or the Security Simulation interface, add the following lines to the dsi.env file for each of those servers:

      ```
      GSK_KEYRING_FILE={Path to the KEYRING FILE}
      GSK_KEYRING_STASH={Path to the KEYRING STASH file}
      GSK_KEY_LABEL=Cert for SelfSigned Server
      ```

CA Chorus for Storage Management Job Submission

5. Submit the following CA Chorus for Storage Management jobs:

   a. E4HI0006 and E4HI0007 in *custom_hlq*.CE4HJCL (Creates the Storage Management interface database USS file system (CE4HVDB))

      Note: If you have an existing CA Chorus system and you want to use the database in a newer CA Chorus version, use the E4HDUPDT job to upgrade the newer system to use the older database.

   b. (Optional) E4HI0008 and E4HI0009 in *custom_hlq*.CE4HJCL (Creates and mounts a USS file system to output Storage Management interface reports). Note the following points before submitting the jobs:

      - If you are using a new system for reporting, run both jobs.
      - If you are using an existing reporting system, run only E4HI0009.

   c. E4HI0010 in *custom_hlq*.CE4HJCL (Identifies storage engine subsystems, creates a password for the Storage Management interface database, and creates an encrypted boot password for the database.)

      Note: If more storage engines are required in the future, this job can be rerun multiple times.

   d. E4HI0011 in *custom_hlq*.CE4HJCL (Configures cost analysis, which is accessible from the Investigator.)

      Note: You can run this job with the default values and then rerun it after you see the objects in the Investigator.

   e. Verify that the TSF configuration is set up. Each storage engine subsystem must be able to connect to the TSF using the loopback address of '127.0.0.1' for an IPV4 stack. To determine if the stack is IPV4 enabled, enter the following command:

      ```
      D TCPIP,stackname,NETSTAT,ROUTE,ADDRTYPE=IPV4
      ```

Finalize the Configuration

6. Submit the following jobs to activate your configuration and start CA Chorus components:

   a. ETJI0105 member in *custom_hlq*.CETJJCL (Configures CA DSI)

   b. ETJI0150 from *custom_hlq*.CETJJCL (Activates your configuration)

      Important! If you are completing this configuration as part of an upgrade, do not start JBoss until you have completed the upgrade procedure. Go to the *Upgrade Guide* now.

   c. Copy the CHORJBOS member to a PROCLIB.

   d. Start the CHORJBOS started task.

   The following message appears when JBoss startup is complete:

   ETJTC001I CA Chorus Startup Complete

7. Go to Verify the Installation and Configuration (see page 48) and then review Post Installation Considerations (see page 50).

   CA Chorus and the applicable disciplines are configured.

Verify the Installation and Configuration

Use this procedure to confirm that you have successfully completed the CA Chorus installation and configuration procedures. If at any point you do not see the expected result, confirm that you have completed the configuration steps as documented. If you cannot identify the issue, contact CA Support.

Note: In addition to this procedure, for CA Chorus for Security and Compliance Management, you can run ETJIVP01 in *chorussec_custom_hlq*.CETJJCL to verify the discipline installation.

Follow these steps:

1. Confirm that the applicable back-end products are up and running.
2. Open a supported browser.

3. Enter the JBoss host name and port in the URL using *one* of the following formats:

   `http://jbosshostname:httpconnectorport/Chorus`
   `https://jbosshostname:httpsconnectorport/Chorus`

   Note: If you ran ETJI0110 in *chorus_runtime_hlq*.CETJJCL to enable HTTPS, use the previously shown HTTPS format to specify the host name and port.

   jbosshostname

   Host name of the system where JBoss is running. Use the value of the TEIID_MACHINE environment variable in CETJOPTN(ENVETJ).

   httpconnectorport

   Port number that is used to access JBoss. Use the value of JBOSS_HTTP_PORT in CETJOPTN(ENVETJ). By default, this value is the TEIID_PORT value +4 for HTTP. For SSL, use the value of JBOSS_SSL_PORT in CETJOPTN(ENVETJ). By default, the value is the TEIID_PORT value + 10.

   Press Enter.

   The CA Chorus login page opens.

   Note: If HTTPS is enabled, follow the prompts to add the URL as a trusted site.

4. Log in to the product.

   The CA Chorus interface opens.

5. Add the Investigator module to your dashboard from the Module Library, and click Start New Investigation.

   The Investigator opens.

6. Select your discipline from the drop-down list in the upper left corner.

7. Confirm that the table in the Investigator displays data.

   You have confirmed that you can log in to CA Chorus and back-end data appears in the user interface.

8. (Optional) Open the Quick Links module, and select a link.

   You have confirmed that the quick links configuration is accurate.

   CA Chorus and the applicable disciplines are installed, deployed, and configured.

Post-Installation Considerations

Before allowing users to access the product, consider the following points:

- Confirm that your mount points and APF authorizations are in your PARMLIB.
- Place your mount points in BPXPRM*xx*.
- If you had to set the MAXFILEPROC, place it in BPXPRM*xx*.
- If you used a customized ETJI095*x* job, copy it to *chorus_runtime_hlq*.CETJJCL.
- If you installed CA Chorus solely to use the SDK, see the *Software Development Kit User Guide* to configure your kit.

Important! For CA Chorus for Storage Management, complete the following procedures to finalize the configuration:

1. Configure the Cost Analysis (see page 79): This procedure is required only if you used CA Chorus Software Manager to configure CA Chorus for Storage Management.
2. Initialize and Configure the Storage Management interface (see page 79): This procedure is required if you configured CA Chorus for Storage Management using CA Chorus Software Manager or the automated method.

Important! For CA Chorus for Security and Compliance Management, complete Configure the Global Configuration (see page 89) to finalize the configuration. Doing so lets the Policy Administration interface send alerts to the Alerts module.

Appendix A: USS Directories

The CA Chorus infrastructure uses the following UNIX System Services (USS) directories:

/cai/cetjr3m0

Specifies the default mount point for CETJZFS0 (read/write zFS).

Note: We recommend that all zFS file systems be permanently mounted by including them in the SYS1.PARMLIB(BPXPRM*xx*) member.

/cai/cetjr3m0/bin

Contains SMP/E-delivered binaries and specialized subdirectories, which also contain SMP/E-delivered binaries.

/cai/cetjr3m0/bin/documentation

Contains CA Chorus documentation and index binaries.

/cai/cetjr3m0/bin/lib

Contains CA Chorus delivered shared objects (DLLs).

/cai/cetjr3m0/CA_axis2c

Specifies the directory where CA_axis2c is installed by default. This directory contains subdirectories and links for data sources processing.

/cai/cetjr3m0/database

Specifies the H2, storage, and custom database top-level directories.

/cai/cetjr3m0/documentation

Specifies the default documentation directory. This directory contains subdirectories and symbolic links pointing to the CA Chorus documentation and indexes.

/cai/cetjr3m0/logs

Specifies the default location for all CA Chorus log files.

/cai/cetjr3m0/userdoc

Specifies the default zFS mount point for user documentation that is uploaded to the Knowledge Center.

/cai/cetjr3m0/utilities

Contains symbolic links to CA Chorus utilities and scripts and output produced by both.

/cai/cetjr3m0/jboss/standalone/tmp

Specifies the temporary directory for USS/CA Chorus files.

Appendix B: Installation and Configuration Troubleshooting

For general troubleshooting, see the *Troubleshooting Guide*.

JBoss Startup Fails Due to Missing File

Symptom:

I used CA CSM to install, deploy, and configure CA Chorus. When I try to do so, it does not start, and I receive an error message indicating a missing file.

This issue is possible for all three configuration methods (CA CSM, automated configuration, and manual configuration).

Solution:

You may have remnants of a previous deployment, which can prevent JBoss from starting.

Follow these steps:

1. Edit and submit FIXLINKS from *your_chorus_hlq*.CETJJCL.
2. Start JBoss.
3. If the problem persists, contact CA Technical Support.

Query Timeout

Symptom:

The query that was executing did not complete in the specified time limit. The following exception occurred:

```
org.teiid.jdbc.TeiidSQLException: Operation timed out before completion.
      at
org.teiid.jdbc.StatementImpl.sendRequestMessageAndWait(StatementImpl.java:935)
at org.teiid.jdbc.StatementImpl.executeSql(StatementImpl.java:484)
```

The timeout value is specified in seconds. The default is 5 minutes (DqueryTimeout=300).

Solution:

Contact CA Technical Support.

USS Files Unavailable

Symptom:

The UNIX System Services (USS) files that were mounted during CA Chorus Software Manager installation are no longer available.

Solution:

Edit member ETJMOUNT in *your_chorus_hlq*.CETJJCL as described in the member to remount the CA Chorus zFS files.

Note: We recommend that all zFS file systems be permanently mounted by including them in the SYS1.PARMLIB(BPXPRM*xx*) member.

Set JBoss Port Assignments Manually

Symptom:

Either of the following symptoms occurs:

- The port range starting with TEIID_PORT in CETJOPTN(ENVETJ) is not acceptable. Twelve consecutive port numbers are not available for the JBoss server ports. ETJI0105 in CETJJCL cannot be used to configure the JBoss port values automatically. Set specific port values.
- For a particular function, the port assignment that is based on the offset from the port that is specified for the TEIID_PORT is not acceptable. Assign this function to a different port.

Solution:

Individual port assignments can be modified by updating ENVETJ in *your_chorus_hlq.*CETJOPTN.

Follow these steps:

1. For the first situation, find as large a range of consecutive free ports as possible. For the ports that are beyond the range available, set the specific port values as shown in Step 2. You can determine which ports are outside the range you have selected by reviewing the OFFSET variable values that are defined in ENVETJ in *your_chorus_hlq.*CETJOPTN.

2. Set the specific port values in CETJOPTN(ENVETJ). For example, to use 45554 for the JBOSS_HTTP_PORT, change the following line:

   ```
   Let JB0SS_HTTP_P0RT=${TEIID_P0RT}+${JB_HTTP_P_0FFSET}
   ```

   To:

   ```
   JB0SS_HTTP_P0RT=45554
   ```

   The port variables that can be modified are:

   - TEIID_PORT
   - JBOSS_HTTP_PORT
   - JBOSS_AJP_PORT
   - JBOSS_SSL_PORT
   - JBOSS_RMI_PORT
   - JBOSS_OSGI_MGMT_PORT
   - JBOSS_TXN_REC_ENV_PORT
   - JBOSS_TXN_STA_MGR_PORT
   - JBOSS_MGMT_NATIVE_PORT
   - JBOSS_MGMT_HTTP_PORT
   - JBOSS_MGMT_HTTPS_PORT
   - JB_RELATIVE_SSL_PORT
   - JB_RELATIVE_AJP_PORT
   - DSI_PORT

3. If you modify the value of JBOSS_HTTP_PORT or JBOSS_SSL_PORT, also modify the value of JB_RELATIVE_SSL_PORT. The new value must be the difference between the value that is assigned for JBOSS_SSL_PORT and JBOSS_HTTP_PORT.

4. If you modify the value of JBOSS_HTTP_PORT or JBOSS_AJP_PORT, also modify the value of JB_RELATIVE_AJP_PORT. The new value must be the difference between the value that is assigned for JBOSS_HTTP_PORT and JBOSS_AJP_PORT.

5. If you modify the value of DSI_PORT, you cannot use ETJI0105 to configure the DSI configuration files. Edit the following files manually to change the default DSI server port assignment:

   Note: The sample dsi.env and dsi.conf files can be taken from directory /cai/cetjr3m0/CA_axis2c/config.

   a. Edit the dsi.env file as follows:

      - Change the directory name in the PATH and LIBPATH variables from /cai/cetjr3m0 to the value specified for <chorus-install-directory>.
      - Change the SYSTCPD_DSN specifies in RESOLVER_CONFIG to match the TCPDATA value in the ETJVARS member in *your_chorus_hlq*.CETJJCL.

   b. Edit the dsi.conf file to specify the TCP/IP port number that you want to use.

   Note: Do not make any other alterations in these files unless explicitly instructed to do so by CA Technical Support.

Set TSF Port Assignments Manually

Symptom:

Access to the TSF relay monitor port is blocked due to site security restrictions. Set a specific port value.

Solution:

Set a value for the TSF relay monitor port (MONPORT parameter) in the TSFRPRMS member in *your_chorus_hlq*.CETJOPTN.

Permission Denied Errors

Symptom:

Permission denied errors appear in the JBoss log.

Solution:

Rerun ETJI0100 in *your_chorus_hlq.*CETJJCL with the user-specified name of the JBoss started task.

Hardware Encryption Error (CHORJBOS Does Not Start)

Symptom:

The following hardware encryption error is received:

Caused by: com.ibm.crypto.hdwrCCA.provider.JCECCARuntimeException: Hardware error from call CSNBRNGL returnCode 16reasonCode 4 com.ibm.crypto.hdwrCCA.provider.SecureRandom.engineNextBytes (SecureRandom.java:104)
java.security.SecureRandom.nextBytes(SecureRandom.java:287)

The CA Chorus JBoss server does not start.

The default java.security that is in use for the JVM contains a provider definition that cannot be supported by the hardware.

Solution:

This problem can be remedied by following these steps:

1. Copy the java.security file from its default location in $JAVA_HOME/lib/security to the CA Chorus directory $INSTALL_HOME/config.
2. Edit the copy of java.security in $INSTALL_HOME/config as follows:

   Note: This file is in EBCDIC format.

   a. Locate the following entry in the list of security provider definitions in this file.

      ```
      security.provider.2=com.ibm.crypto.hdwrCCA.provider.IBMJCECCA
      ```

      Note: The index number may be different.

   b. Delete the line that you located in the previous step, and adjust the index numbers of the remaining security.provider entries accordingly.

   c. Save the edited file.
3. Edit the ENVETJ member of the CA Chorus CETJOPTN data set as follows:

   a. Insert the following line immediately above export IBM_JAVA_OPTIONS="$IJO":

      ```
      IJO="$IJO
      -Djava.security.properties=${INSTALL_HOME}/config/java.security"
      ```

   b. Save the edited file.

Error During Security Discipline Reconfigure Using E1MI0010 or E1MI0020

Symptom:

I am attempting to reconfigure CA Chorus for Security and Compliance Management and I am using the same high-level qualifier and UNIX System Services (USS directory). When I try to rerun E1MI0010 or E1MI0020, I get a return code of 0 or 1280. However, I see errors in STDOUT that indicate a velocity permission issue.

Solution:

To resolve this issue, set the velocity log permissions to 664. This log resides *your_runtime_home*/logs.

Error During Security Discipline Reconfigure Using E1MI0014

Symptom:

I am attempting to reconfigure CA Chorus for Security and Compliance Management, and I am using the same high-level qualifier and UNIX System Services (USS directory). When I try to rerun E1MI0014, the jobs fails due to *your_runtime_home*/config permission problem.

Solution:

To resolve this issue, set the nodetype_config.xml permissions to 775. These config.xml files reside in *your_runtime_home*/config.

Example:

chmod 775 *your_runtime_home* /config/acf2_config.xml

chmod 775 *your_runtime_home* /config/cmgr_config.xml

chmod 775 *your_runtime_home* /config/tss_config.xml

Use ETJICUST to Point to Another Deployment

Symptom:

I have different deployments with only modest customization values differences. How can I use ETJICUST to point to another deployment.

Solution:

You can make your changes in the same Configuration_ds file. Doing so saves you time and reduces the likelihood of errors.

1. Make a copy of an existing configuration file.
2. Modify this file (most likely, you will change SMS, port, and the Run_time HLQ).
3. Run ETJICUST with this configuration file and the new <Output_ds_HLQ>.

Appendix C: CA Chorus Installation Worksheet

Use this worksheet to record CA Chorus values specified at your site during installation and configuration and values that you must know in advance.

Installation Data Sets

The following values were specified during installation and deployment of the CA Chorus product packages (pax files). These values are reused for discipline installations.

CA Chorus high-level qualifier

Specifies the high-level qualifier where the CA Chorus data sets are defined.

HLQ for zFS File System

Specifies the high-level qualifier (HLQ) to use for the CA Chorus zFS file systems. This value can be the same value used for the target libraries, the default, or a different HLQ.

Java Home Directory

Specifies the USS directory (without a trailing forward slash) where Java is installed. This directory contains the /bin directory and other files. CA Chorus requires IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0 Service Release 2,5 or 7 (5655-W44) or IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 1 (5655-W44), including optional JZOS batch launcher.

Default: /sys/java64bt/v7r0m0/usr/lpp/java/J7.0_64.

JAVALIB

Specifies the fully qualified data set name of the PDS/E that contains the JVMLDMnn module that is installed with JZOS, which is a feature of IBM Java.

Default: MVSSYS.JAVA64BT.V7R0M0.SR2.SIEALNKE

USS Target Directory Name

Specifies the target directory path where CA Chorus is installed. CA Chorus Software Manager mounts a zFS file system in this location so the directory must be a valid USS file system mounting point. If the directory does not exist, it is created. If it exists, it must be an empty directory without any file systems mounted to it.

Default: /cai/cetjr3m0

USS Group Name

Specifies the default USS group (YOURGRP) of the user that is installing CA Chorus.

Note: From OMVS, use the **id** command from USS to list the user ID through your security system. For example, the IBM default OMVSGRP is a common value for this field.

Ports

Use this worksheet to record the values that are specified for the CA Chorus ports. These values are specified during the CA Chorus configuration:

JBoss Server Ports

Specifies the beginning port assignment for the 12 consecutive port values that are required by the CA Chorus JBoss server started task (CHORJBOS by default). There is not a default for the 12 consecutive ports.

Use the TEIID_PORT setting in the ENVETJ member of *your_chorus_hlq.*CETJOPTN to specify the ports.

Important! For various discipline configuration tasks, you may need to know the CA Chorus port.

httpconnectorport

Port number that is used to access JBoss. Use the value of JBOSS_HTTP_PORT in CETJOPTN(ENVETJ). By default, this value is the TEIID_PORT value +4 for HTTP. For SSL, use the value of JBOSS_SSL_PORT in CETJOPTN(ENVETJ). By default, the value is the TEIID_PORT value + 10.

Time Series Facility (TSF)

Specifies the TSF region port values for the CHORTSF started task. Three ports are required.

Use the TSFPARMS member in *your_chorus_hlq.*CETJOPTN to set the three TSF region ports.

Time Series Facility Remote Relay

Specifies the TSF remote relay port values for the CHORTSFR started task. Two ports are required.

Use the TSFRPRMS member in *your_chorus_hlq.*CETJOPTN to set the two TSF remote ports.

Note: The TSF Remote Relay uses a third port for monitoring the connection from the TSF relay to the TCP/IP stack. By default, this port is dynamically allocated. To specify this port value instead of having it dynamically allocated, edit the MONPORT parameter in the TSFRPRMS member in *your_chorus_hlq*.CETJOPTN.

CA Chorus for Storage Management Quick Links module display port

Specifies a display port number in the CHORWEBX started task and in CETJOPTN(ENVE4H) for the -DDISPLAY variable. One port is required.

One of the last steps after configuring the post CA Chorus for Storage Management is to start the CHORWEBX started task so that the Quick Link Storage Management interface can create charts. Assign this port within TCP/IP to the CHORWEBX task. The CHORWEBX task is located in CE4HJCL(E4HWEBX).

JBoss Environment Variables (ENVETJ)

The ENVETJ member in *chorus_runtime_hlq.*CETJOPTN contains the configuration information for the JBoss server that must be edited to set site-specific environment variables. The variables are described in the ENVETJ member, but additional information is provided here for your reference.

INSTALL_HOME

Specifies the mount point for the USS target directory &CAI.CETJZFS0. Set to the same value specified for USS target directory during CA Chorus Software Manager installation. For example, /u/chorus.

Default: /cai/cetjr3m0

JAVA_HOME

Specifies the location of the JDK (directory where Java is installed). Set to the same value that was specified for Java Home DIR during the CA Chorus Software Manager installation. For more information, see Installation Data Sets (see page 61).

TEIID_PORT

Specifies the lowest of 13 consecutive port numbers that are assigned for Teiid JDBC access using ETJI0105 in *chorus_runtime_hlq.*CETJJCL. Confirm that all ports in the specified range are not already in use and can be reserved for use by the CA Chorus JBoss server.

If you configure ports manually, follow the instructions in the ENVETJ member (see CA Chorus Ports (see page 62)).

Range: TEIID_PORT to TEIID_PORT+11

TEIID_MACHINE

Specifies the server name (host name or the IP address) where the JBoss server is running. This value indicates the CA Chorus machine name.

DSI_RESOLVER

Specifies the data set name that is defined to SYSTCPD in the TCP/IP started task on the system. Replace <SYSTCPD_DSN> with the value specified for TCPDATA in the ENVETJ member of *chorus_runtime_hlq.*CETJOPTN.

Default: TCPIP.TCPIP.DATA

Example: DSI_RESOLVER="TCPIP.TCPIP.DATA" or DSI_RESOLVER="TCPIP.TCPIP.DATA(*membername*)"

Note: If the EZB.STACKACCESS resource is protected, the appropriate READ permissions are needed for the CA Chorus ID that is associated with JBoss.

Important! This value is not used for real-time Compliance Information Analysis (CIA) in CA Chorus for Security and Compliance Management. Do *not* alter this value as part of configuring CIA.

DSI_JOBNAME

(Optional) Specifies the z/OS job name that appears on the console for the CA DSI process that is spawned from the CA Chorus server. If a value is not specified, the job name is the same as the CA Chorus server job name. If the job name is less than eight characters, the job name is the same as the CA Chorus server job name with a numeric suffix.

To use a specific name for the DSI job, uncomment the option #export DSI_JOBNAME="" in ENVETJ and insert a new job name for the DSI job in between the quotation marks.

Note: This variable is ignored if the CA Chorus server user does not have BPX.SUPERUSER authority.

Important! This value is not used for real-time Compliance Information Analysis (CIA) in CA Chorus for Security and Compliance Management. Do *not* alter this value as part of configuring CIA.

DSIDMPHLQ

Specifies the high-level qualifier (HLQ) under which a dump for the CA DSI Server is captured. This HLQ is substituted in the dsi.env file that is created in the ETJI0105 job to collect diagnostic information at runtime.

Replace <HLQ-of-dump-dataset-for-DSI-Server> in DSIDMPHLQ="<HLQ-of-dump-dataset-for-DSI-Server>" with your value to capture a dump for CA DSI Server.

Limit: No more than 21 characters

Example: DSIDMPHLQ="DSI.DUMP"

The dump data set is in the form DSI.DUMP.Dxxx.Txxxxxxx.Pxxxxxxx.

JAVA_DUMP_TDUMP_PATTERN

Specifies the name of the JVM SYSDUMP output data set where dump data sets are created. Replace <JDMPHLQ> with the data set high-level qualifier (HLQ).

Note: The JBoss server task needs security permissions to write to the data sets under the specified HLQ.

Dmaster.pds

Specifies the data set name where the report templates are stored. This value must match the name specified for EZT_MASTER_PDS in the ENVEZT member of *your_chorus_hlq.*CETJOPTV.

MAX_ALERT_LIMIT

Specifies the maximum number of alerts that are stored for CA Chorus for Security and Compliance Management and CA Chorus for Storage Management. After the maximum number of alerts is reached, CA Chorus deletes the oldest alert and stores the new one. The value that is specified applies to both disciplines. For example, if the value specified is 1000, CA Chorus stores 1000 security alerts and 1000 storage alerts.

Default: 5000

Appendix D: Additional CA Chorus for DB2 Database Management Configuration

Override the DB2 Execution Mode

To support a DB2 subsystem running in Compatibility Mode (CM or CM*), you update a user configurable file to reflect the current executing mode of DB2. The configuration file directs CA Chorus for DB2 Database Management to treat a DB2 subsystem running in CM or CM* as a different version of DB2. This file is located in the following USS directory and is created as part of deploying CA Chorus for DB2 Database Management:

`/<chorus-install-home>/roles/dba/DBMzDB2-version-override.txt`

Note: This procedure assumes that the applicable CA Chorus servers are already defined.

Follow these steps:

1. Add a DB2 subsystem override definition in comma-separated value (CSV) format for each DB2 running in CM or CM* using the E3KMOD10 member in *your_chorusdba_hlq*.CE3KPARM. The file is comma-separated value (CSV) format and contains the following columns:

   dsConf

   Specifies the confederation that is used to access this DB2 subsystem. The confederation names are defined in the db2tools.cfg configuration file that is located in the /cai/cetjr3m0/CA_axis2c/config USS directory by default.

   dsGroup

   Specifies the DB2 data sharing group attach name. If the DB2 subsystem is not a data sharing group member, leave this value blank.

   dsSystem

   Specifies the LPAR where the DB2 subsystem is running.

dsSSID

Specifies the DB2 subsystem identifier.

VersionOverride

Specifies the DB2 override version. Use the following values in place of the actual DB2 version.

- For DB2 V8, specify 081.
- For DB2 9, specify 091.
- For DB2 10, specify 101.

2. Copy the E3KJBCRD member in *your_chorusdba_hlq.*CE3KJCL into the EK3I0030 member in *your_chorusdba_hlq.*CE3KJCL, save your changes, and submit the job.

   The CA Chorus for DB2 Database Management DB2 subsystem version override definitions are created. The DBMzDB2-version-override.txt file in <chorus-install-home>/roles/dba is updated.

3. Activate your changes by restarting the CA Chorus JBoss STC.

Example:

In this example, note the following DB2 subsystem settings:

- DA0G and D91A are part of the QA confederation as defined in the db2tools.cfg.
- DA0G is a DB2 10 data sharing group member of data sharing group DA0G running in CM9.
- D91A is a DB2 10 subsystem running in CM8*. The DB2 subsystem is not a data sharing group member.

To support this configuration:

1. Update the E3KMOD10 member as follows:

```
dsConf,dsGroup,dsSystem,dsSSID,VersionOverride

QA    ,DA0G   ,CA31    ,DA1G  ,091
QA    ,       ,CA31    ,D91A  ,081
```

2. Submit the E3KI0030 member in *your_chorusdba_hlq.*CE3KJCL.

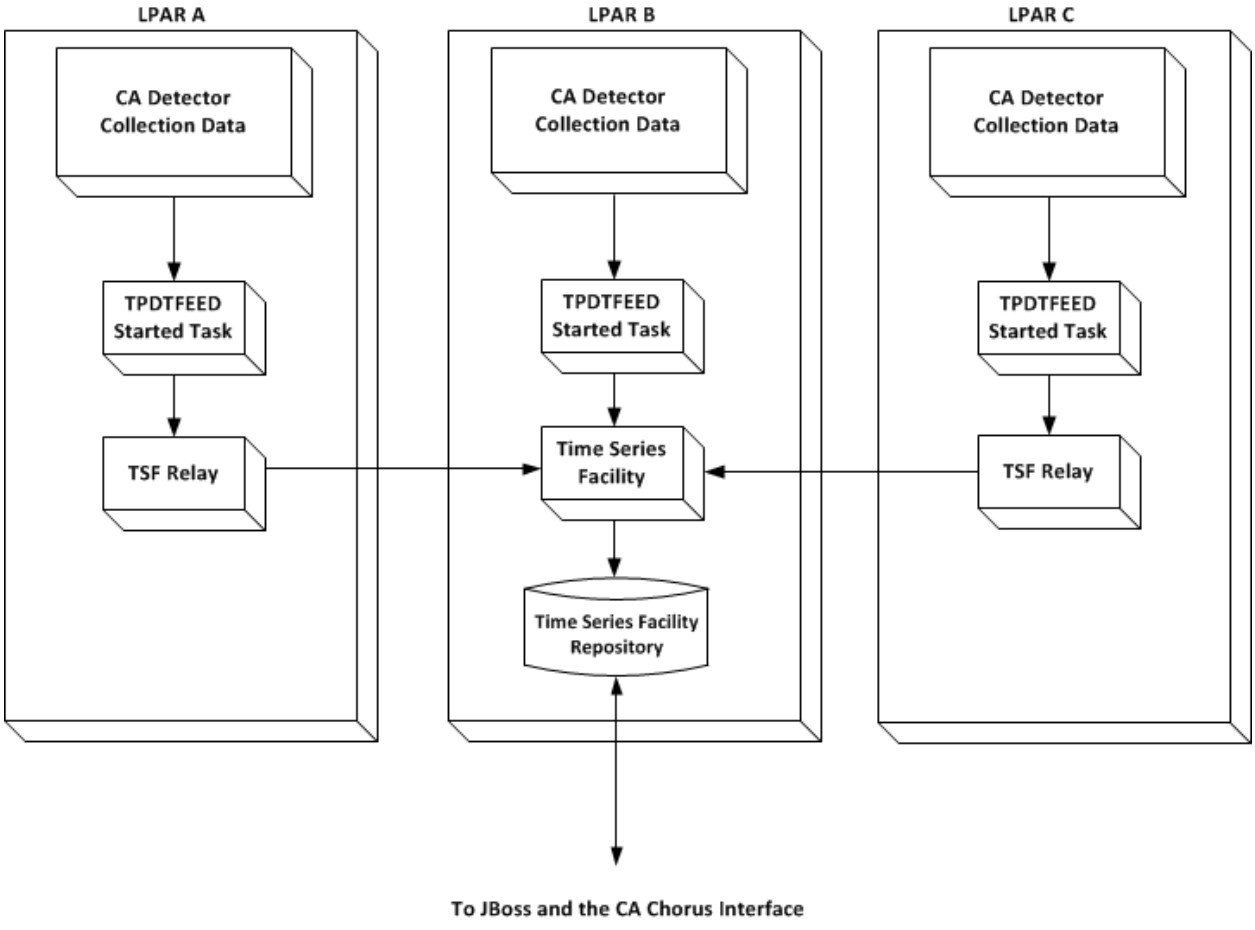
CA Detector Statistics Gathering Overview

The Time Series Facility (TSF) displays application performance data in CA Chorus. Before you can view application performance data using TSF, start statistics gathering in CA Detector. Statistics gathering is the process of collecting system statistics and sending data to TSF for a specific time frame (collection interval).

Note: This configuration is not required for integration with CA Chorus Infrastructure Management for Networks and Systems.

Important! This step must be performed manually outside of CA Chorus Software Manager.

The following diagram shows the statistics gathering configuration for a single enterprise:



In the previous diagram, CA Detector passes collection data automatically from each DB2 subsystem being monitored (LPAR A, B, and C) to TSF when a collection interval ends using the TPDTFEED started task. The TSF relay passes data to TSF from remote LPAR A and C. TSF saves the data in the TSF repository.

- To load CA Detector collection data to TSF automatically, complete the following steps:

  1. Customize and submit the TPDTCOPY batch job in *your_db2tools_hlq*.CDBASAMP.
  2. Customize the TPDTFEED started task in *your_db2tools_hlq*.CDBASAMP.
  3. Automate the started task using CA OPS/MVS or another message processing and scheduling service. (REXX EXEC TPDT0170 is provided in in *your_db2tools_hlq*.CDBASAMP.)

- To load CA Detector collection data manually when an automation service like CA OPS/MVS is not available, use the TPDTHIST batch job in *your_db2tools_hlq*.CDBASAMP.

How to Load CA Detector Collection Data Automatically

Use the following process to provide CA Detector collection data automatically to the Time Series Facility (TSF) in CA Chorus.

The TPDTFEED started task procedure runs the CA Detector UNLOAD utility for the most recently completed CA Detector collection interval on a DB2 subsystem. This started task also provides that data to the Time Series Facility (TSF) through a TCP/IP connection. The task is executed for each CA Detector collection interval per DB2 subsystem.

When a collection interval ends, message PDT0170 is issued in the Xmanager JOBLOG where the collection is running. Use this message to trigger the start of each TPDTFEED started task.

Note: If CA OPS/MVS is not available, another message processing and scheduling service can be used.

Follow these steps:

1. Edit and submit the TPDTCOPY member in *your_db2tools_hlq*.CDBASAMP as described in the member.

   Note: Select a CA Detector TSF high-level qualifier (TPDTHLQ) that determines where to create the CA Detector TSF parmlib and unload data sets. TPDTHLQ must not exceed a length of 12 characters to avoid exceeding the 44 character DSN limit.

   The CA Detector TSF parmlib library is created and the TPDTPARM member is copied to the new library.

Alternatively, use the following definitions to create the CA Detector TSF parmlib data set manually, and then copy the member TPDTPARM from *your_db2tools_hlq*.CDBASAMP to *TPDTHLQ*.PDTTSF.PARMLIB:

```
DISP=(NEW,CATLG,DELETE),DSNTYPE=LIBRARY,UNIT=SYSDA,
DCB=(RECFM=FB,LRECL=80,BLKSIZE=3120,DSORG=PO),
DSN=TPDTHLQ.PDTTSF.PARMLIB,SPACE=(TRK,(100,20))
```

2. Verify that the following required permissions are provided for the z/OS ID used to start the TPDTFEED started task:
   - OMVS segment for TCP/IP
   - READ access to the high-level qualifier of the CA Database Management Solutions for DB2 for z/OS
   - UPDATE access to the chosen CA Detector TSF high-level qualifier (TPDTHLQ)

   The TPDTFEED started task required permissions are defined.

3. Customize the TPDTFEED started task:
   a. Copy the TPDTFEED member in *your_db2tools_hlq.*CDBASAMP to a PROCLIB.
   b. Edit the TPDTFEED member as described in the member. The PRDTSF step transmit data to TSF.
   c. Ensure that the CA Detector collection interval is set to a valid TSF interval. The TSF interval is restricted to 1, 5, 10, 15, 20, or 30 minutes or to 1, 2, 4, 6, 8, 12, or 24 hours.

      Note: For more information about specifying these collection intervals, see the *CA Detector User Guide*.

4. Customize the REXX EXEC TPDT0170:

   a. Copy the TPDT0170 REXX EXEC located in *your_db2tools_hlq*.CDBASAMP into a valid CA OPS/MVS production rule set. This EXEC processes data collector messages from Xmanager and starts the TPDTFEED started task that provides data to TSF. A sample message follows:

      ```
      PDT0170 DETECTOR COLLECTION INTERVAL END TIME=08:00
      INTERVAL=01:00 DB2=ssid VCAT=PDTDBA.Rnn
      DATASTORE=datastore-name
      ```

      Note: If CA OPS/MVS is not available, another message processing and scheduling service can be used.

   b. Edit TPDT0170 as follows:

      - Modify the site-specific variables for active subsystems and Xmanager jobs.
      - Under tsf_jobname<1-3>, set the TPDTFEED STC names and the corresponding release of the CA Database Management Solutions for DB2 for z/OS.

      Note: If multiple releases send data to TSF concurrently, define a separate TPDTFEED STC for each release.

5. (Optional) See Seeding Data to Multiple TSF Regions to send data to TSF regions on multiple CA Chorus installations.

How to Load CA Detector Collection Data Manually in Batch

CA Detector history data can be fed to the Time Series Facility (TSF) in batch using the TPDTHIST job that is located in *your_db2tools_hlq*.CDBASAMP. Use the TPDTHIST batch job in *your_db2tools_hlq*.CDBASAMP to load data into TSF manually.

Follow these steps:

1. Create the history collection file using the CA Detector UNLOAD utility.

   Note: For help using the CA Detector UNLOAD utility and the batch reporting facility, see the *CA Detector for DB2 for z/OS User Guide*.

2. Edit the member TPDTHIST in *your_db2tools_hlq*.CDBASAMP as described in the member.

3. Submit the member.

   Member TPDTHIST is updated and executed.

Sending Data to Multiple TSF Regions

If you have multiple installations of CA Chorus, complete the following steps to transmit data to multiple Time Series Facility (TSF) regions:

Note: These steps are not needed unless you want to send data from a given DB2 subsystem to more than one CA Chorus installation. For information about concurrent versions with TSF, see the *Upgrade Guide*. For information about remote TSF systems, see the *Manual Configuration Guide*.

1. Copy the TPDTFEED STEP PRDTSF in the TPDTFEED started task directly underneath the original PRDTSF step, and specify a new STEPNAME. For example:

```
//*-------------------------------------------------------------
//PRDTSF   EXEC PGM=PDTTSF,REGION=0M,COND=(4,LE,UNLOAD),
// PARM='-I&ITIME &ETIME'
//STEPLIB  DD  DISP=SHR,DSN=&TGTPFX..CDBALOAD
//INFILE   DD  DISP=SHR,
//             DSN=&TPDTHLQ..PDTTSF.DB2&SSID..D&VDATE..T&VTIME
//SYSOUT   DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//SYSERR   DD  SYSOUT=*
//STDERR   DD  SYSOUT=*
//CEEDUMP  DD  SYSOUT=*
//*-------------------------------------------------------------
//OTHERTSF   EXEC PGM=PDTTSF,REGION=0M,COND=(4,LE,UNLOAD),
// PARM='-I&ITIME &ETIME'
//STEPLIB  DD  DISP=SHR,DSN=&TGTPFX..CDBALOAD
//INFILE   DD  DISP=SHR,
//             DSN=&TPDTHLQ..PDTTSF.DB2&SSID..D&VDATE..T&VTIME
//SYSOUT   DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//SYSERR   DD  SYSOUT=*
//STDERR   DD  SYSOUT=*
//CEEDUMP  DD  SYSOUT=*
```

2. Specify the additional TSF region using a unique value for the TSFSUFFIX parameter (-T) in the PARM statement. This value must match TSFSUFFIX of the TSF region you are connecting to. For example, to start a second TSF region with a TSFSUFFIX of O, specify -TO as follows:

   ```
   // PARM='-I&ITIME -TO &ETIME'
   ```

   Note: By default, TSFSUFFIX (-T) is not required.

3. Save your changes to the TPDTFEED started task.

   In this example, the OTHERTSF step connects to the TSF region with a TSFSUFFIX of O. This region runs on the same LPAR as the TPDTFEED started task executes.

How to Enable DB2 Object Migration

Before you can use the Object Migrator function in CA Chorus for DB2 Database Management to migrate DB2 objects, perform the tasks in the following procedure manually outside of CA Chorus Software Manager. This procedure creates the OFA configuration PDS and members, updates the OFAPROC started task JCL, and updates the MJETJOM model JCL.

Note: This configuration is not required for integration with CA Chorus Infrastructure Management for Networks and Systems.

Note: To execute the Batch Processor, you must be granted EXECUTE authority on the Batch Processor plan. For more information about granting product authorizations, see the *CA Database Management Solutions for DB2 for z/OS General Facilities Reference Guide*.

Follow these steps:

1. Confirm that at least one CA RC/Migrator utility model ID exists.

   Note: The @DEFAULT model is created during CA RC/Migrator post-installation DB2 catalog customization. Confirm that an @DEFAULT model exists for CA RC/Migrator. You can create this model and additional models using the CA RC/Migrator profile option (PROF). Select Utility Model Services, and then use the template (T) option to create a model using an existing model as a template. For more information about creating models, see the *CA RC/Migrator User Guide*.

2. Allocate a configuration PDS with the following attributes for use by the Object Framework Services agent (OFA):

   Note: The OFA is created and customized during post-installation processing of the CA Database Management Solutions for DB2 for z/OS. For more information about post-installation processing, see the *CA Database Management Solutions for DB2 for z/OS Implementation Guide*.

   - Tracks: 2
   - Record format: FB
   - Record length: 80
   - Block size: 27920

   The OFA configuration PDS is allocated.

3. Define global configuration parameters:

   a. Create the default global configuration member (@DEFAULT) in the OFA configuration PDS.

   b. Add the following JCL:

```
<JOB CARD>
//jobcard JOB (ACCT INFO),'job title',CLASS=A,MSGCLASS=X,
//       MSGLEVEL=(1,1),REGION=0M,NOTIFY=userid
</JOB CARD>
<MODEL4>
MODEL4 model ID
</MODEL4>
<MODEL4C>
MODEL4C creator
</MODEL4C>
```

   c. Replace the italicized text with site-specific values. Include the desired JOB statement for z/OS batch jobs (<JOB CARD>, </JOB CARD), the model ID or name (<MODEL4>, </MODEL4), and creator (<MODEL4C>, </MODEL4C>).

   d. Save your changes.

      The @DEFAULT global configuration member is created.

   Important! By default, the DBA Command Manager and Object Migrator functions will create temporary work data sets using the TSO PREFIX of each user as the high-level qualifier. You can override the default settings as described in Step 4.

4. (Optional) To specify an alternate high-level qualifier for use with temporary work data sets:

   a. Create a member in the OFA configuration PDS for each Object Migrator user that is named the same as their user ID. You can use the @DEFAULT member in the OFA configuration PDS as a template.

      Note: Use the JOB statement, model name (ID), and creator values for overriding global settings. The model ID and creator must match the members that you create. The creator specifies the member creator user ID.

   b. Add the following tags:

      ```
      <SYSTEM:lpar>
      <PREFIX>
      hlq;
      </PREFIX>
      </SYSTEM:lpar>
      ```

   c. In this JCL, specify the LPAR name (*lpar*) and the high-level qualifier (*hlq*) to be used with the creation of temporary work data sets for this user.

      Note: The *hlq* must be terminated with a semi-colon.

      For example:

      ```
      <SYSTEM:LPAR1>
      <PREFIX>
      MYPREFIX.CHORUS;
      </PREFIX>
      </SYSTEM:LPAR1>
      ```

      Note: For more examples of overriding high-level qualifiers for work data set allocations, see the *CA Chorus for DB2 Database Management User Guide*.

   d. Save your changes.

      The user member is created.

   For example:

   When you are done adding members, the members appear in the configuration data set members list. These members are used during DB2 object migration when the migration is submitted for analysis. The user members override global settings that are defined in the @DEFAULT member.

5. Update the OFAPROC started task JCL:

   Notes:

   - The OFAPROC started task is created and customized during configuration of the Object Framework Services agent (OFA). For more information about configuring the OFA, see the *CA Database Management Solutions for DB2 for z/OS Implementation Guide*.
   - The OFAPROC started task ID needs READ permission for BPX.SERVER.
   - If the EZB.STACKACCESS resource is protected, the appropriate READ permissions are needed for the user ID associated with the OFAPROC started task and the users requesting access to the Object Migrator function.

   a. Add the CFGFILE and SYSTCPD DD statements.

      ```
      //CFGFILE  DD DISP=SHR,DSN=config.om.pds
      //SYSTCPD  DD DISP=SHR,DSN=&tcpdata
      ```

      config.om.pds

      Specifies the name of the PDS that was previously created for the Object Migrator configuration.

      &tcpdata

      Specifies a TCPDATA data set from SYSTCPD of TCPIP PROC.

      Default: TCPIP.TCPIP.DATA

   b. (Optional) If you want to direct output to a data set instead of SYSOUT (the default):

      - Add the following DD statements for the sequential log data sets:

        //LOGGER1 DD DISP=SHR,DSN=*hlq*.LOGGER1

        //LOGGER2 DD DISP=SHR,DSN=*hlq*.LOGGER2

      - Allocate the sequential log data sets manually with the following attributes:

        Record format: VB

        Record length: 1028

        Block size: 6144

        Cylinders: 20.

      Note: To turn off the logging capability for OFAPROC, contact CA Support for instructions.

   Save your changes.

   The OFAPROC started task JCL is updated.

   Note: Enable these changes by recycling the agent.

6. Update the MJETJOM model JCL member in *your_db2tools.hlq*.CDBAMDL as follows:

   a. (Optional) If you are using JES3, replace the /*JOBPARM S=%SYSTEM statement with //*MAIN SYSTEM=%SYSTEM.

   b. Set %CHRPFX to the high-level qualifier prefix for the CA Chorus target library data set name prefix (*hlq.*CETJPLD). This value must match the value that is specified during the installation of CA Chorus.

   c. Add the following DD statement for the TCPDATA data set name to all steps executing FLQMASTT:

      ```
      //SYSTCPD   DD DISP=SHR,DSN=&tcpdata
      ```

      &tcpdata

      Specifies a data set from SYSTCPD of TCPIP PROC.

      Default: TCPIP.TCPIP.DATA

   Save your changes.

   The MJETJOM model is updated and Object Migrator is configured for use in the CA Chorus Investigator.

Appendix E: Additional CA Chorus for Storage Management Configuration

Configure the Cost Analysis

If you used CA Chorus Software Manager to configure CA Chorus for Storage Management, you must manually configure Cost Analysis.

Note: If you used the Automated Configuration method to configure CA Chorus for Storage Management, you do not need to perform this procedure.

Follow these steps:

1. Submit the E4HI0011 job from *custom_hlq*.CE4HJCL. (This configures Cost Analysis, which is accessible from the Investigator.)

   Note: You can run this job with the default values and then rerun it after you see the objects in the Investigator. For more information about changing the Cost Analysis variable values to better fit your site at a later time, see the *Administration Guide*.

2. Submit the ETJI0150 job from *custom_hlq*.CETJJCL (This activates your configuration.)

   The Cost Analysis objects display data in the Investigator.

Initialize and Configure the Storage Management Interface

CA Chorus for Storage Management customers must initialize and perform some Storage Management interface configuration so users can use it. The following items must be done:

- A name for the single-signon authenticating host for the Storage Management interface must be specified.
- A display port must be specified so reports can be created from the Storage Management interface.
- The Storage Management interface database must be initialized.
- At least one *public* host for the single-signon authenticating storage engine subsystem for the Storage Management interface must be created.

- Email server settings must be specified.
- The charting facility must be configured.

Note: Some Storage Management interface functions have limited use until the system administrator performs more tasks. For more information about these tasks, see the *Administration Guide*.

Follow these steps:

1. Edit and submit the ENVE4H member in *your_chorus_hlq*.CETJOPTN as described in the member. All of the Storage environment variables can run with the supplied default values except the <*vantage_public_host*> variable in the following statement:

   ```
   #IJO="$IJO –Dvantage.web.client.host.name=<vantage_public_host>"
   ```

   Note: If you have started the CA Chorus JBoss task, restart it to activate the environment variable changes by issuing the following commands:

   ```
   /P CHORJBOS, to stop it
   ```

   ```
   /S CHORJBOS, to start it
   ```

2. Log in to CA Chorus.
3. Add the Quick Links module to your CA Chorus dashboard, and click Manage Storage Resources.

   The Storage Management interface log on window opens in a separate browser window.

4. Enter the system administrator user Name and Password.

   The system administrator credentials are as follows:

   - The default system administrator user Name: APP
   - Password: See the WEBUI_ADMINPASSWORD parameter that is specified in the E4HI0010 job in *your_chorusstor_hlq*.CE4HJCL.

5. Select VantageDB in the Authenticating Host field, and click Login.

   If you are logging in to the Storage Management interface as the system administrator for the first time, the Storage Management interface database starts to initialize.

6. Click OK in the initialize confirmation dialogs that appear.

   After the database initialization completes, the Storage Management interface opens in your browser with the My Profile window open. If the My Profile window does not open, click My Profile in the Storage Management interface Menu bar or select My Profile from the Tools menu.

   Note: The Storage Management interface online help details how to use the different options in the My Profile window.

7. Click Add Host Definition.
8. Enter values and make selections in the New Host Definition dialog for the following required fields:

   Important! Create a single *public* host for users to authenticate for single-sign on using the host that is specified in step 1.a. When a user is logged in to the Storage Management interface, they can create their own *private* hosts.

   Note: New Host Definition dialog field explanations are available in the Storage Management interface online help system.

   Host Name

   Specifies a unique host name. This name appears in the Host Definition List and Object Tree. Consider that you could eventually have multiple hosts. The host names must be equivalent to the *StorageDsName* variables in the E4HI0010 job.

   Important! Create a public host for the single-signon authenticating host that is specified in step 1.a.

   Note: The host name is case-sensitive. Enter the host names exactly as you entered the values for the *StorageDsName* variables in the E4HI0010 job.

   IP Address

   Specifies the IP address where the storage engine z/OS host runs. This value is the same as the value of the *VantageIpAddr* variable in the E4HI0010 job.

   Port

   Specifies the port number of the storage engine z/OS host. This value is the same as the value of the *VantageIpPort* variable in the E4HI0010 job.

   Include On Object Tree

   Select this option so that the Storage Management interface displays the host name in the Object Tree for all end users.

   Use PassTicket

   Select this option. When this option is selected, the following actions occur:

   - The PassTickets security feature is invoked.
   - Automatic log in to the Storage Management interface occurs when end users select the Manage Storage Resources link in the Quick Links module.

   PassTickets do not send the password over the network, instead the PassTicket configuration on the host is used. PassTickets must be activated on *each* storage engine host for this option to work.

   Note: For more information about activating PassTickets on the storage engine hosts, see the *CA Chorus for Storage Management Site Preparation Guide*.

Public Host

Select this option. At least one *public* host is required for CA Chorus for Storage Management. However, if you are using multiple storage engine subsystems for your CA Chorus user-interface, create a *public* host for each subsystem.

Note: This option is only available if you are logged in as the system administrator to the VantageDB database.

Note: Do not define *private* hosts when logged in as the system administrator to VantageDB if you plan to activate PassThrough in the *private* host definition. Users can activate PassThrough in their *private* host definitions. Use the Storage Management interface online help to learn how to use the different My Profile options to create their *private* hosts after they open the Storage Management interface from the Quick Links module.

9. Click OK.

   The My Profile window opens with the *public* host definition in the Host Definition List. The Scope column should read "PUBLIC".

   A *public* host is created for the *StorageDsName*: ADDR(*VantageIpAddr*) PORT(*VantageIpPort*) (first) line that you have in the E4HI0010 job. This single *public* host is required for users to authenticate for single-sign on using the host that is specified in step 1a.

10. (Optional) Create more public hosts for each additional storage engine subsystem that is set up for your CA Chorus user-interface by repeating steps 7 through 9. This step is for creating public host definitions for the remaining *StorageDsName*: ADDR(*VantageIpAddr*) PORT(*VantageIpPort*) lines that you have in the E4HI0010 job.

    Note: This step is marked optional because it is easier to perform it now while you are logged on to the Storage Management interface as a system administrator. You also have the additional hosts information from the E4HI0010 job. However, the system administrator can add new and can manage existing *public* hosts any time. For the instructions, see the *Administration Guide*.

11. Test that the *public* Host Definitions work for the Storage Management interface from the My Profile dialog:

    a. Select the newly created *public* Host Definition in the Host Definition List.

    b. Click Actions, and then Connect.

       The login dialog opens.

    c. Enter a valid User Name and Password for the *public* host. The User Name and Password must have the access authority to the storage engine on the z/OS host of the *public* host definition.

    d. Click Log In.

       The *public* host is listed in the Object Tree pane with status *connected*. You have created and tested the *public* host.

e. Repeat steps a through d for each public host definition.

f. Click Close to close the My Profile dialog.

12. Set the Storage Management interface email server settings of the email server the Storage Management interface uses to send emails and set number of concurrent reports. Follow these steps:

    In this context, the email server is the email server the Storage Management interface uses to send emails to the following items:

    - The output report recipients.
    - Email failure notices if the reports are not produced (for example, as scheduled).

    Note: Output report schedules and request for a failure notification are maintained using the Customize Report Wizard by the end user.

    a. Click Tools in the Storage Management interface Menu bar and then Application Configuration to open the Application Configuration dialog.

    b. Specify email server settings.

       The email Server pane in the Application Configuration dialog has the following options:

       Email Server

       (Required) The DNS name or IP address of your email server, which the Storage Management interface uses to relay email messages. The Storage Management interface sends email directly to the recipient email server using the SMTP protocol.

       Port

       (Required) The port number of the email server that the Storage Management interface uses to send emails.

       The Storage Management interface sends emails for the following items:

       - Report emails with output report attachments.

       - Report generation failure messages.

       The default value is 25. However, some sites use a different value, for example, 587.

       User Name

       (Optional) Enter the user ID that has the authority to send email from the designated email server. This field is for sites that have the security requiring an authorized user ID and password to send email.

       Note: Only enter a user ID if the mail server designated for relaying Storage Management interface email only accepts authorized requests.

Password

(Optional) Enter the password of the user ID that has the authority to send email from the designated email server.

Note: Only enter a password if the mail server designated for relaying Storage Management interface email only accepts authorized requests.

Note: If the Storage Management interface continues to have problems sending email after adding the *Email Server* settings, you have probably encountered a security problem. For example, some corporate firewalls disable or could be configured to disable outgoing connections to port 25 (the SMTP default port). Contact your Email Administrator, Network Administrator, and Security Administrator to discuss the correct values for the Email Server Setting fields. Storage Management interface emails are sent with the sender address of VantageGMIScheduler@ca.com.

13. Verify that the single-sign on authenticating *public* host connection and passticket for the Storage Management interface works from the Quick Links module:
    a. Click Logout in the Storage Management interface toolbar and close the Storage Management interface browser window.
    b. Click Manage Storage Resources in the Quick Links module from your CA Chorus dashboard.

       The Storage Management interface opens in a separate window and logs on automatically.

       Note: If automatic logon is unsuccessful, verify PassTickets are defined properly. For more information, see the *CA Chorus for Storage Management Site Preparation Guide*.
14. Close Storage Management interface and CA Chorus.
15. Configure the charting utility that is used in the Storage Management interface:
    a. Copy the member E4HWEBX from the CE4HJCL library to your proclib.

       This member contains the charting utility started task that is used to create charts in the Storage Management interface. Start the CHORWEBX procedure before the CA Chorus JBOSS started task. Verify with your system administrator that execution permissions are granted on the Xvfb X Server (application) and the Xvfb startXvfb.sh script.

       The JCL is copied and ready for modifications.

b. Follow the instructions in the sample JCL.

   Because this procedure runs as a started task, its JCL procedure must reside in one of your system proclibs.

   Note: The Xvfb application is part of the IBM Ported Tools for z/OS. IBM Ported Tools for z/OS is a nonpriced program product that is designed to deliver tools and applications for the z/OS environment. These applications have been modified to operate within the z/OS environment. IBM Ported Tools for z/OS is only available to customers with a license to z/OS; it is supported on z/OS 1.4 and above. Xvfb is an X server that can run on machines without display hardware and physical input devices. Xvfb emulates a dumb framebuffer using virtual memory. APAR OA10965 provides support for Xvfb. Consult with administrators for the location of the installed application for Xvfb X-Server. For example: /usr/lpp/tcpip/bin/X11/samples directory.

   The STC is now ready for execution.

c. Start the CHORWEBX PROCLIB member for the *Xvfb X* server.

   The *X* server address space starts.

   If the server starts successfully, the following messages appear in STDOUT:

   ```
   Starting Xvfb using server/display: 11
   Xvfb will be run in the background.
   Run "ps -ef | grep Xvfb" to see process ID.
   ```

   If the startup fails, the following message appears in STDOUT:

   ```
   XVFB0178: Failed to establish all listening sockets
   ```

   The *Xvfb X* server JOB is completed.

   The CHORWEBX is started.

d. Start CHORMUF, CHORTSF, and CHORJBOS in this order by issuing the following commands:

   ```
   /S CHORMUF
   /S CHORTSF
   /S CHORJBOS
   ```

   You receive a confirmation message after entering each command.

   Note: You must start CHORWEBX before starting the CHORJBOS task.

16. Verify that charting is enabled in the Storage Management interface by doing the following steps:

    a. Log in to CA Chorus.

    b. Click Manage Storage Resources in the Quick Links module from your CA Chorus dashboard.

       The Storage Management interface opens in a separate window and logs on automatically.

c. Open any object in the Storage Management interface. For example, the Space and Other Attributes object in the Storage Groups folder of the Object Tree.

d. Click Customize Settings to open the Customize View Wizard.

e. Click Chart in the Navigation Tree of the Customize View Wizard.

f. Click the check-box next to Show Chart, and click Finish.

A line chart with default settings is displayed in the Storage Management interface. You have verified that charting is enabled in the Storage Management interface.

g. Click Log Out in the Storage Management interface Menu bar, close the browser window, and log out of the CA Chorus user-interface.

The following Storage Management interface initialization and configuration items are completed:

- A name for the authenticating single-signon storage engine subsystem for the Storage Management interface is specified.
- The Storage Management interface database is initialized.
- A display port is specified so that charts can be created from the Storage Management interface.
- At least one *public* host for the authenticating single-signon storage engine subsystem is configured.
- Email server settings are specified.
- The charting facility is configured.

Note: The Storage Management interface system administrator can do the following tasks any time:

- Create new and manage existing Storage Management interface *Public* Hosts.

  Note: Users can manage their Storage Management interface global options. For more information, see the *CA Chorus for Storage Management User Guide*. Users can also create their own Storage Management interface *private* host definitions when they are logged on to the Storage Management interface.
- Stop and Start the Storage Management interface Scheduler.
- Manage Storage Management interface scheduled items.
- Create new and manage existing Storage Management interface *public* logo images.
- Create new and manage existing Storage Management interface *public* holiday schedules.

- Create new and manage existing Storage Management interface *public* user views of source objects.

For more information about these tasks, see the *Administration Guide*.

Appendix F: Additional CA Chorus for Security and Compliance Management Configuration

Configure the Global Configuration

Configure the global configuration to specify Policy Administrator settings.

Follow these steps:

1. Add the CHORUS CETJPLD library to the steplib in the Compliance Manager Monitor and Alert PROCS.
2. Stop and re-start both address spaces before proceeding to the next step.
3. Add the Quick Links module to a dashboard.
4. Click Administer Compliance Policy.

   The Policy Administrator UI opens.
5. Click the applicable instance from the Administration pane.

   The tree expands to show the folders.
6. Click Policy Administration, Configuration.

   The Configuration window opens.
7. Type the CA Unicenter web address, your CA Unicenter user ID, password, and then confirm your password under Service Desk.

   The service desk settings are set.
8. Type the DLL file name *libedb2* in the module field under Change Control.

   The change control setting is set.
9. Type the CA Chorus host, port, password, connection type, log location, and log level under Alert.

   The Chorus Alerts are configured.
10. Select the Weekend/Weekday Designation from the drop-down list.

    Weekends and weekdays are defined.

11. (Optional) Specify the default WTO Route Code and Descriptor Code Designation.

    The default settings for WTO are specified.

12. Click Create Configuration.

    A confirmation message appears.

Global Configuration Pane

The Global Configuration pane lets you manage the global settings for the Service Desk account, change control, email servers, CA Chorus alerts, weekend/weekday designations, and WTO route code/descriptor code designation.

The Global Configuration pane contains the following fields:

Service Desk

Includes the fields to identify the service desk and the user.

URL

Defines the address of CA Unicenter where the Policy Administrator sends service desk notices.

Example: http://*yourserver.com*:*port*/axis/services/R11_USD_WebService

Userid, Password, Confirm

Defines your CA Unicenter ID and password. When service desk notices occur, the Policy Administrator associates the service desk ticket with this user ID.

Change Control

Includes change control options.

Module

Defines the data link library (DLL).

Email

Includes email options.

Primary Email Server

Defines the URL of the primary email server.

Primary Email Server Port

Defines the port of the primary email server.

Backup Email Server

Defines the URL of the backup email server.

Backup Email Server Port

Defines the port of the backup email server.

Alert

Includes the CA Chorus Alert options.

Machine Name for Alerts

Defines the server name that the CA Chorus alert is sent to. This value is defined under TEIID_MACHINE in the ENVETJ member in *chorus_runtime_hlq*.CETJOPTN.

Example: yourserver.com

Port for Alerts

Defines the port on the server where the CA Chorus alert is sent.

Example: 7070

The following definition details the CA Chorus port:

httpconnectorport

The port number that is used to access Jboss. Use the value of JBOSS_HTTP_PORT in CETJOPTN(ENVETJ). By default, this value is the TEIID_PORT value +4 for HTTP. For SSL, use the value of JBOSS_SSL_PORT in CETJOPTN(ENVETJ). By default, the value is the TEIID_PORT value + 10.

Host URL

Indicates the full URL that the CA Chorus alert is sent to. This noneditable field is displayed if you have specified machine name and port for alerts.

Example: http://yourserver.com:7070/Chorus/services/eventListener

Username, Password, Confirm

Defines the name and password of the user for HTTP authentication.

Connection Type

Specifies the connection type (Basic Authentication or PassTicket Authentication).

Default: Basic Authentication

Log Location

Defines the path to the file containing the log for the alert session.

Log Level

A numeric value indicating the level of logging.

Weekend/Weekday Designation

Weekend

Specifies two days that are considered the weekend.

Weekdays

Indicates the nonweekend days that are considered weekdays.

Default WTO Route Code/Descriptor Code Designation

Includes the WTO message default options. The numerical values have different meanings and can be used differently across organizations. If you are unsure of the value to use, contact your System Programmer.

Default Descriptor Code

Specifies the descriptor code that is assigned to the WTO messages sent by the Policy Administrator.

Default Route Code

Specifies the default routing code that is used for the WTO messages sent by the Policy Administrator.