CA Chorus™

Administration Guide

Version 03.0.00, Sixth 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 DPM)
- 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 ([set the rcm variable for your book])
- 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 fifth edition of this documentation:

- How to Promote a Test System (see page 95)—Noted that CAMFC resource class and entries cannot be modified.
- Configure the Global Configuration (see page 145) and Global Configuration Pane (see page 146)—Updated these topics to reflect changes to the Compliance Manager Policy Administration UI.

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

- How to Log Metrics Panel Data (see page 93)—Added this topic to describe how to log Metrics panel data in the server.log file.

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

- Back Up the H2 Database (see page 65) and Restore the H2 Database (see page 70)—Added new procedures to back up and restore the H2 database.

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

- Disable Automatic Configuration of Heap Memory (see page 31)—Added new procedure to disable the automatic configuration of heap memory.
- How to Change the Log Level for All Executions (see page 91)—Renamed this procedure (formerly titled *How to Change the Log Parameters)* and removed chorus.logservice properties, which are not supported in 3.0.
- How to Change the Log Level Temporarily (see page 92)—Renamed this procedure for clarity (formerly titled *How to Change the Log Level*).
- Start CA DSI (see page 21)—How to start CA DSI.

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

- Legal Notices (see page 2)—Updated to reflect public documentation legal disclaimer.
- How to Promote a Test System (see page 95)—Added this scenario.
- Discipline Specific Administration Tasks (see page 75)
  - Added a new procedure to change Cost/Value field values in the Customer Site Costs Data object, using the Investigator is added to the section How to Change the Cost Analysis Configuration (see page 77). (PTF RO63077 required.)

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

- Global—Changed all references of ENV in *chorus_runtime_hlq.*CETJOPTN to ENVETJ.
- How to Authorize Users to Work in CA Chorus—Moved this scenario to the *Site Preparation Guide*.
- Global CA Datacom/AD changes
  - Explained that CHORMUF is a variable and you should use your MUF name in commands.
  - Clarified that the MUF is a CA Datacom/AD MUF.
- Start CA Chorus Components (see page 13)
  - Added a warning that you must start the components in the order noted and must wait for each component to start before moving to the next start command.
  - Changed wording from servers to components for technical accuracy.
  - Changed CA Chorus for DB2 Database Management Object Framework Services (OFA) agent name from F2OFAAGT to OFAPROC. This update applies to the start and stop commands.
- Start CA Chorus Infrastructure Management for Networks and Systems Components
  - Added a note about starting CA NetMaster NM for TCP/IP before CA Chorus at startup.
- Managing CA Chorus Components (see page 13)
  - Added procedures to start and stop back-end components for all disciplines.
- Customize the Teiid Timeout Value (see page 31)
  - Updated steps 1 and 2 for 3.0 behavior.
  - Explained how to disable the timeout.
- Reinitialize the CA Chorus Database (see page 45)—Added this topic.
- Reinitialize the Time Series Facility Database (see page 46)—Added this topic.
- Time Series Facility Database Requirements (see page 46)
  - Added note that Areas G01/2/3/4 have Auto Dynamic Extend enabled by default.
  - Added note about MultiVolume INITs.
- TSF Database Recommendations (see page 47)—Added this topic, including recommendations for each discipline.
- How to Customize the Time Series Facility Database (see page 57)
  - Added options for CA SYSVIEW and CA NetMaster NM for TCP/IP to supply data for CA Chorus Infrastructure Management for Networks and Systems.

- Added automation recommendations.
- Added more detail and number of metric management examples.

- Increase Data Set Space Allocations (see page 55)
  - Simplified this procedure to show one method to increase allocations.
  - Clarified the jobs and the sequence in which you run them.
  - Added details about TSDB102, which deletes the TSF database in the MUF.
  - Clarified the definition of TSDB002, which allocates and defines the TSF database to the MUF.
  - Removed the steps to stop and start the CA Datacom/AD MUF. The MUF must be active.
- How to Implement HA Automatic Restart Management (see page 33)
  - Noted the Automatic Configuration option to enable High Availability.
  - Noted the new security job name and that security requirements now reside in the *Site Preparation Guide*.
- Modify the Started Task JCL for the ARM Wrapper (see page 42)
  - Noted the Automatic Configuration option to enable High Availability.
  - Modified steps 1 and 2 to account for 3.0 behavior.
  - Noted that TSF Data Relay Return Codes now reside in the *Troubleshooting Guide*.
- Discipline Specific Administration Tasks (see page 75)—Added CA Chorus for Storage Management Administration Tasks, which includes:
  - How to Add or Remove Storage Engines
  - New step 6 added to the instructions (see page 75): 6. Submit either the $TJI0150 or ETJI0150 job in CETJJCL to update the data source XML files with the storage engines.
  - How to Change the Cost Analysis Feature Configuration
  - How to Change Topology Viewer Configuration
  - How to Administer the Storage Management Interface
  - How to Manage Storage Management Interface Public Hosts
  - How to Manage Storage Management Interface Email Server Settings and Number of Concurrent Reports
  - How to Stop and Start the Storage Management Interface Scheduler
  - Additional Storage Management Interface Administrator Tasks

Contents

Chapter 1: Managing CA Chorus Components

How to Start CA Chorus

Before you start using the CA Chorus web service application, ensure that the started tasks required for the configuration of CA Chorus are active on all of your systems. You can start the CA Chorus and discipline-related components independently.

Start the CA Chorus Components

The CA Chorus web services infrastructure includes the database Multi-User Facility (MUF), JBoss server, and Time Series Facility. This infrastructure is typically started on only one system in your configuration. These servers cooperate to provide the entry point for CA Chorus users.

Start the CA Chorus components in the order that is shown in the following procedure. Some dependencies exist in the startup sequence as noted in the procedure.

Note: We recommend that you automate this procedure as much as possible. This information helps you restart the configuration.

Important! Start these components in the order noted. Do not continue with the next start command until you have confirmed that the current server has started.

Follow these steps:

1. Start the CA Datacom/AD database MUF by entering the following console command:

   S *your_muf_name*

   The following messages appear:

   - Message DB00212I appears on the z/OS console to identify the release of CA Datacom/AD that you have installed.
   - Message DB00201I appears on the z/OS console to indicate the MUF is up.

2. Start the Time Series Facility (TSF):

   S CHORTSF

   A message indicating that TSF is initialized is logged.

   ```
   N00503 *** TSF INITIALIZATION COMPLETE TSF ***
   ```

3. Start the TSF Relay, if you are using a relay for remote LPARs:

   ```
   S CHORTSFR
   ```

   A message indicating that TSFR is initialized is logged.

   ```
   N00503 *** TSF INITIALIZATION COMPLETE TSF ***
   ```

4. Start the JBoss server:

   ```
   S CHORJBOS
   ```

   A message indicating that startup is complete is logged.

   ```
   ETJTC001I CA Chorus Startup Complete
   ```

Start CA Chorus for DB2 Database Management

Start the CA Database Management Solutions for DB2 for z/OS and the CA Chorus for DB2 Database Management products on each system in your CA Chorus for DB2 Database Management configuration.

The startup sequence that is shown in this section is a logical sequence. You can start and stop the products independently. The products create logical connections to each other based on the XMANID startup parameter that is specified for each product. The Xmanager and Xnet combine to provide cross-memory and network connectivity for the other products. Xnet automatically connects to Xmanager when it is available. When Xnet and Xmanager are available and connected, the CA Chorus agents in the other products automatically connect to make their services available to authorized CA Chorus users.

Follow these steps:

1. Start Xmanager by entering the following console command:

   ```
   S PTXMAN
   ```

   Message PXM0101 is logged when initialization is complete. The CA Chorus agent for CA Detector and CA Subsystem Analyzer runs in the Xnet address space. This agent starts automatically when Xnet connects to Xmanager.

2. Start Xnet by entering the following console command:

   Note: TCP/IP must be up before starting Xnet.

   ```
   S PXNPROC
   ```

   Following are the results of this command:

   - Message xntDRV050I PASSNAME(*applname*) is logged to show the application name configured for PassTicket verification.
   - Message xntXNT002I Xnet-Xmgr connected XMANID *xmanid* pxnv *pxnv-addr* is logged when Xnet successfully connects to Xmanager.

- Message xntDRV002I CA Xnet initialization complete - Release nn.0.0 is logged when Xnet initialization is complete.
- Message xntTCP904I Listener: PXNWTSS host address ::0 and port *nnnn* is logged when the Xnet TCP/IP listener is ready to receive CA Chorus requests from the CA Chorus web server.

3. Start the CA Insight DPM program call owner:

   S IDB2PC

   Message DBG39046I *tver hh:mm:ss* INITIALIZATION IS COMPLETE FOR PC OWNER TASK is logged when program call owner initialization is complete.

4. Start CA Insight DPM data collectors by entering the following console command for each DB2 subsystem being monitored:

   S *db2ssid*DC

   db2ssid

   Identifies the DB2 subsystem ID.

   Message DBG39044I *ssid hh:mm:ss* INITIALIZATION IS COMPLETE FOR DATA COLLECTOR FOR DB2 SUBSYSTEM *ssid* is logged when data collector initialization is complete.

   The agent connects to the CA Chorus configuration when Xmanager and Xnet are active and connected. Diagnostic message *mm/dd/yy hh:mm:ss.tht* Xnet Agent up id(*agent-id*) xmgr(*xmanid*) is logged to the data collector job log when the data collector is ready for CA Chorus request processing.

5. Start the Object Framework Services agent (OFA):

   S OFAPROC

   The agent connects to the CA Chorus configuration when Xmanager and Xnet are active and connected. The following messages are logged to the OFS agent job log to indicate that the agent is up and ready to service CA Chorus requests:

   ```
   ETJOF002I: XMAN  ID: XXXX

   ETJOF003I: AGENT ID: XXXXXXXXXXXXXXXX

   ETJOF800I: OFA INITIALIZATION COMPLETE
   ```

Start CA Chorus Infrastructure Management for Networks and Systems Components

For CA SYSVIEW, go to How to Specify the Start Mode on the Started Task (see page 16).

For CA NetMaster NM for TCP/IP, go to Start the SOLVE SSI Region.

Note: We recommend that you start the focal point CA NetMaster NM for TCP/IP region to which CA Chorus connects before CA Chorus is started. Post CA Chorus startup, if necessary, you can restart the region without needing to restart CA Chorus.

How to Specify the Start Mode on the Started Task

You can specify the start mode when you start the Main Services address space started task.

Specify the start mode using one of the following three methods:

- Method 1: Issue the following START command for the started task:

  ```
  S SYSVIEW,START=COLD
  S SYSVIEW,START=WARM
  ```

- Method 2: Use the following command START= parameter within the started task PROCLIB member:

  ```
  //SYSVIEW PROC MEM=SYSVIEW,START=WARM
  .
  .
  //SYSVIEW EXEC PGM=GSVXMAIN,REGION=0M,TIME=1440,
  //         PARM='&MEM,&START'
  .
  ```

- Method 3: Specify as an initialization option in the parmlib member specified by the MEM= parameter. The default member name is SYSVIEW:

  ```
  WARM
  or
  COLD
  ```

Start CA NetMaster NM for TCP/IP SOLVE SSI Region

Start the SOLVE SSI region by issuing the following command from the MVS console:

S *ssiname*,REUSASID=YES

ssiname

Specifies the name that you specified for the SOLVE SSI during the CA NetMaster NM for TCP/IP setup process.

Note: If you use cross memory services, specifying REUSASID=YES makes the address space ID of a terminated SOLVE SSI reusable. Otherwise, the ID is unavailable until after the next IPL.

Proceed to Start the CA NetMaster NM for TCP/IP Region (see page 17).

Start the CA NetMaster NM for TCP/IP Region

To start the region, issue the following command:

S *rname*,REUSASID=YES

rname is the name that you specified for the region during the CA NetMaster NM for TCP/IP setup process.

Note: If you use cross memory services but do *not* specify REUSASID=YES, and the region terminates, the address space ID is not available until after the next IPL.

Note: To stop the started task, issue the following command from the MVS console: P *rname*.

Start CA Chorus for Security and Compliance Management Components

Select the following procedures based on your configuration.

Start CA ACF2

After you configure CA ACF2, you can start the product.

Before starting CA ACF2, verify the following:

- CAIRIM is installed. (CAIRIM is part of the CA Common Services.)
- The TSO procedure IKJACCNT is available. This procedure is the default used for your initial signon with the default user ID and default GSO TSO options.

Follow these steps:

1. Start CA ACF2 using one of these methods:

   - If you want to start CA ACF2 automatically and you have edited the CAISECXX member of CAI.CAACF.PARMLIB as described in CA ACF2 System Initialization, do the following:

     - Copy CAISECXX from CAI.CAACF.PARMLIB into the CAISEC*xx* member of SYS1.PARMLIB.

     - Copy the CAIACFXX member from CAI.CAACF.PARMLIB into the CAIACF*xx* member of SYS1.PARMLIB. It contains the CA ACF2 startup parameters.

     You can proceed to item #3 at this point.

   - If you want to start CA ACF2 manually, add the S ACF2 command to the COMMND*xx* member of SYS1.PARMLIB. Because CA ACF2 runs as a subsystem, it should be fully initialized before you process any job with JES2 or JES3.

2. Construct the initial set of Global System Options (GSO) records.

   During the initial IPL, CA ACF2 attempts to locate GSO records. When CA ACF2 detects that no records are present, it prompts the operator for continuation options as shown in the following sample. Reply as indicated to construct the initial set of GSO records. Subsequent CA ACF2 startups do not require operator intervention.

   ```
   ACF79505 INITIAL START IN PROGRESS FOR SYSTEM: sysid
   ACF79510 WARNING: NO GSO RECORDS FOUND FOR SYSTEM: sysid
   *10 ACF79517 CONTINUE GSO PROCESSING WITH DEFAULT VALUES?
   reply 10,u
   ACF79530 NO GSO RECORD FOUND FOR: recid SYSID: sysid
   *11 ACF79534 CONFIRM USE OF DEFAULTS FOR: recid SYSID: sysid
   reply 11,u
   ACF79507 GSO PROCESSING COMPLETED WITHOUT ERROR
   ```

   If you are migrating from a prior version, changes or additions to GSO options can result in warning message ACF79600, which indicates that the record is outdated. This message is normal. Change the records flagged to set the new or changed option as appropriate for the site. Refresh the GSO record to put the option into effect.

   Note: When a new field is added to an existing GSO record, the value of the new field is not necessarily the default value specified in the documentation. This is because when a new field is added to an existing GSO record, the new field assumes the value that is in the area of the record that it now represents. To ensure the default values are used for new fields, the record must be inserted by the current version of CA ACF2.

3. Start JES.

   JES2 needs only a warm start. JES3 requires a hot start.

4. Start TSO and log on to the system as ACFUSER or the site-specified logonid supplied in job INITIAL.

5. Complete the following if you have a shared DASD environment.

   The CA ACF2 GSO BACKUP record should include the CPUID parameter to identify the single system responsible for backup processing. You can use the NOBACKUP parameter of the S ACF2 command to deactivate automatic backup processing on a given system. BACKUP is the default. For more information, see the chapter "Maintaining Global System Options Records" in the *Administrator Guide*.

You no longer need to identify the CA ACF2 subsystem name in IEFSSN*xx* in SYS1.PARMLIB. CA ACF2 intercepts the system security initialization module and dynamically installs its own subsystems by building subsystem control table (SSCT) entries.

Start CA Top Secret

CA Top Secret can be started:

- As a subsystem before JES. Specify SUB=MSTR on the O/S START command. TYPE=2 (or JES2) and LEVEL=SP n.n.n must be specified in the JES control option. Failure to do so displays the message TSS9112E-UNABLE TO DETERMINE JES LEVEL.
- During a system IPL after JES initialization. Start CA Top Secret *before* all of the CA Common Services except CAIRIM. CAIRIM must initialize before CA Top Secret.

If the TSS address space is up before JES, the $$$LOG$$ spool file is automatically allocated when JES starts. For CPF nodes that require sysout support, the nodes will need to be defined in the NDT and refreshed after JES is up. Spool files for those nodes will then be allocated without restarting the TSS address space. Because of this change, TSS must shut down before JES.

Note: If a subsystem with the same name as a started task exists, the MSTR subsystem is the default for the started task. If no MSTR subsystem exists, the primary JES subsystem is used. In CA Top Secret r15, we established a subsystem with the name TSS. Therefore, if the procname that starts CA Top Secret is TSS, it will start under the master subsystem. To avoid the procname running under MSTR, change the name of the proc.

How to Initialize CA Top Secret as a Subsystem

This section explains how to use CAISEC00 to start CA Top Secret and CA SAF SECTRACE subsystems automatically. You can initialize CA Top Secret from CAISEC00 or from the command table SYS1.PARMLIB(COMMNDxx).

Note: For first-time installations of CA Top Secret, put a START TSS entry in SYS1.PARMLIB(COMMNDxx) or a TSS(xx START) entry in CAISEC00; otherwise, you must start CA Top Secret manually from the operator console.

1. Create a member called CAISEC00 for your started tasks. In CAISEC00, list each subsystem name, whether it should start automatically, and which members of SYS1.PARMLIB contain additional operands for the START command. For example:

   ```
   EDIT ---- SYS1.PARMLIB(CAISEC00) - 01.01 -------------- COLUMNS 001 072 COMMAND
   ===> SCROLL ===> CSR
   ************************ TOP OF DATA ************************ 00000001 TSS(xx
   START)
   00000003 TRCE(xx START)
   00000004 PROMPT
   ************************ BOTTOM OF DATA ************************
   ```

   Note: To start some, but not all, of the subsystems listed in the CAISEC00 member, place an asterisk (*) to the left of the name of each subsystem that you do not want to start. Notice that the entry number matches the SYS1.PARMLIB member. For example, TSS(01 START) matches member CAITSS01.

2. Specify the following keyword in the CAISEC00 member. To do so, selecting the CAISECxx suffix by responding to the prompt message:

   PROMPT

   Indicates that the operator console should be prompted for specification of the CAISEC initialization parameters. During CA SAF initialization, a WTOR message CAS2070I is issued to allow the operator to specify the CA SAF initialization parameters.

3. Specify that CA SAF is to use the CAITSSxx parmlib member by using one of the following options:

   ```
   TSS(xx)
   TSS(xx START)
   TSS(xx NOSTART)
   ```

4. Specify the CAISECxx parmlib member suffix by using one of the following options:

   `SEC=xx or SEC(xx)`

   This step lets a site maintain multiple CAISECxx parmlib members. CAISEC00 is the initial parmlib member processed during CA SAF startup processing. Within the CAISEC00 member, you can specify any of the valid initialization parameters, including SEC=xx to indicate that an alternate parmlib member should be processed. The last value processed for any of the valid initialization keywords is the value selected for processing. To avoid initialization processing loops, a CAISEC member suffix can be specified only once for processing.

   Note the following behaviors:

   - To use the CAISEC00 parmlib member as it currently exists, use the U option to cause CA SAF. This value is the default, and it lets you continue processing.
   - The U option is available as a response to the prompt at the console only; you cannot use it as a keyword value in CAISEC00. You are unable to specify any other parameters after you specify U.
   - If you specify a single parameter or multiple parameters, such as TSS(xx), these replace their counterparts in CAISEC00 or any other CAISECxx member that you specify with the SEC(xx) parameter. All other parameters remain the same.

   Note: To use one or more of these options automatically at startup, put them in CAISEC00 and remove the PROMPT keyword.

Start the CA LDAP Server

At this point, the product is deployed and configured. You are ready to start up the CA LDAP Server.

1. Copy the LDAPR151 STC PROC from CDT9JCL into your proclib.
2. Start the STC using the LDAPR151 job.

CA LDAP is now started on your system.

Start CA DSI

At this point you are ready to start CA DSI.

1. Copy the DSIR151 STC PROC from SAMPJCL into your proclib.

   The DSIR151 STC PROC is in your proclib.

2. Start the STC using the DSIR151 job.

Start the CA Compliance Manager Components (Manually)

The CA Compliance Manager components that you chose to implement must be started and active so that the security events from the external security manager (ESM) can be processed through the Router and received by the active components and updated.

The following started task procedures are used to start the CA Compliance Manager components:

- CMGRRTR - starts the Router component (required)
- CMGRLOGR - starts the Logger component
- CMGRWHSE - starts the Warehouse component
- CMGRMON - starts the Monitor component
- CMGRALRT - starts the Alert component

Important! The Router must be started and active before any of the other components can start receiving events.

Follow these steps:

1. Copy all the CA Compliance Manager started task procedures from the CAI.CEIQPROC library into the library from which the procedures will be executed (for example, SYS1.PROCLIB).
2. Modify and configure the started task procedures to conform to your installation standards. Specify the logstream name and the DB2 subsystem (ssid) or CA Datacom/AD MUF name (CMGRMUF). For more information, see the CA Compliance Manager *Implementation Guide*.
3. Start the Router by issuing the following console command:

   ```
   S CMGRRTR
   ```

4. Verify that the Router successfully started.
5. Start the Logger component, if you are implementing a Data Mart repository, by issuing the following console command. Otherwise, skip this step:

   ```
   S CMGRLOGR
   ```

6. Verify that the Logger component successfully started.

   If the Router is not active, CA Compliance Manager prompts you to start the Router. Retry component initialization by responding 'Y' to the following prompt:

   ```
   CMGR220I CMGR Retry Initialization <Y> or <N> ?
   ```

   Issue the following status operator command to view Logger component status:

   ```
   F CMGRLOGR,STATUS
   ```

7. Start the Warehouse component, if you are implementing a Warehouse, by issuing the following console command:

   ```
   S CMGRWHSE
   ```

8. Verify that the Warehouse component successfully started.

   If the Router is not active, CA Compliance Manager prompts you to start the Router. Retry component initialization by responding 'Y' to the following prompt:

   ```
   CMGR220I CMGR Retry Initialization <Y> or <N> ?
   ```

   Issue the following status operator command to view Warehouse component status:

   ```
   F CMGRWHSE,STATUS
   ```

9. Start the Monitor component, if you are implementing a Monitor repository, by issuing the following console command:

   ```
   S CMGRMON
   ```

10. Verify that the Monitor component successfully started.

    If the Router is not active, CA Compliance Manager prompts you to start the Router. Retry component initialization by responding 'Y' to the following prompt:

    ```
    CMGR220I CMGR Retry Initialization <Y> or <N> ?
    ```

    Issue the following status operator command to view Monitor component status:

    ```
    F CMGRMON,STATUS
    ```

11. Start the Alert component by issuing the following console command:

    ```
    S CMGRALRT
    ```

12. Verify that the Alert component successfully started.

    If the Router is not active, CA Compliance Manager prompts you to start the Router. Retry component initialization by responding 'Y' to the following prompt:

    ```
    CMGR220I CMGR Retry Initialization <Y> or <N> ?
    ```

    Issue the following status operator command to view Alert component status:

    ```
    F CMGRALRT,STATUS
    ```

Start the CA Compliance Manager Components (Automatically)

You can use the command table in SYS1.PARMLIB(COMMNDxx) instead of the console command to start CA Compliance Manager component address spaces as early as possible during the IPL process, preferably before JESx initialization.

Follow these steps:

1. Copy all the CA Compliance Manager started task procedures from the CAI.CEIQPROC library into the library from which the procedures will be executed (for example, SYS1.PROCLIB).
   - CMGRRTR - starts the Router component (required)
   - CMGRLOGR - starts the Logger component
   - CMGRWHSE - starts the Warehouse component
   - CMGRMON - starts the Monitor component
   - CMGRALRT - starts the Alert component

   Important! The Router must be started and active before any of the other components can start receiving events.

2. Edit the COMMNDxx member in SYS1.PARMLIB to add the following entries for any of the CA Compliance Manager components you chose to implement:

   ```
   COM='S CMGRRTR,SUB=MSTR'
   COM='S CMGRLOGR,SUB=MSTR'
   COM='S CMGRWHSE,SUB=MSTR'
   COM='S CMGRMON,SUB=MSTR'
   COM='S CMGRALRT,SUB=MSTR'
   ```

3. Verify that the CA Compliance Manager components you chose to implement successfully started during the IPL process.

   Issue any of the following status operator command to view component status:

   ```
   F CMGRRTR,STATUS
   F CMGRLOGR,STATUS
   F CMGRWHSE,STATUS
   F CMGRMON,STATUS
   F CMGRALRT,STATUS
   ```

Start the CIA Real-Time Component

After completing the configuration, security definitions, and control options steps, you can start and stop the CIA real-time component.

The following steps describe how to start and stop the CIA real-time component:

- Automatically start during initialization
- Start with a console command
- Stop the CIA real-time component

Note: We recommend that the CIA real-time component address spaces start as early as possible following security product initialization.

Automatically Start During Initialization

The CIA real-time component is automatically started if you defined the proper CIA security definitions and control options earlier in this Guide.

Start with a Console Command

If you did not yet start the CIA real-time component, use a console command to manually start the CIA real-time component.

To manually start the CIA real-time component, issue the following command at the console:

```
S CIARTUPD
```

Note: If you changed the name of the CIA real-time component procedure, specify that value in the command rather than CIARTUPD.

Start CA Chorus for Storage Management Components

To start the host server, issue the following operator START command (but only after JES2 is running):

```
S SAMS
```

The following message confirms that the TCP/IP interface starts properly:

VAN0845I *stcname* Listening on TCP Port: *xxx*

Verify that this message was received.

If the system has problems connecting to the CA TCPaccess stack, contact your CA TCPaccess administrator for assistance. If problems persist or other stack-related questions remain, contact CA Support. Supply the release of CA Vantage SRM being used and the socket interface being used for the connection (HPNS).

How to Stop CA Chorus

You can stop the CA Chorus components independent of the back-end products supporting each discipline. For example, CA Database Management for DB2 for z/OS products that are used with CA Chorus for DB2 Database Management. When the CA Chorus components are down, the back-end products continue to operate in your environment.

Stop the CA Chorus Components

The CA Chorus web services infrastructure is normally active on only one system in your configuration. The infrastructure includes the following:

- JBoss server
- Time Series Facility (TSF)
- TSF Relay
- Database Multi-User Facility (MUF)

Use the following shutdown procedure to stop the components. The dependencies exist in the shutdown sequence are noted in the procedure.

Follow these steps:

1. Stop the JBoss server by entering the following console command:

   P CHORJBOS

   A message indicating that the JBoss server started task has ended is logged.

2. Stop the Time Series Facility (TSF):

   P CHORTSF

   A message indicating that TSF has ended is logged.

3. Stop the TSF Relay, if you are using a relay for remote LPARs:

   P CHORTSFR

   A message indicating that TSFR has ended is logged.

4. Stop the CA Datacom/AD database MUF:

   P *your_muf_name*

   A message indicating that the MUF has ended is logged.

Stop CA Chorus for DB2 Database Management

You can stop and restart each of the CA Database Management Solutions for DB2 for z/OS and CA Chorus for DB2 Database Management independently. If you stop Xmanager, Xnet, or both, the CA Chorus agents in your other products can no longer communicate and provide service to CA Chorus users until Xmanager, Xnet, or both are restarted.

If you are performing a complete shutdown of the products, the following procedure provides a logical order for the shutdown. This logical order can be useful if you are automating a shutdown procedure for the products. Each product can be stopped independent of the other products. If you must shut down a single product, go to that step and issue the appropriate shutdown command. When the product is restarted, it automatically rejoins your network of CA Chorus agents.

Follow these steps:

1. Stop the Object Framework Services agent (OFA) by entering the following console command:

   ```
   P OFAPROC
   ```

   Message ETJOF002I: OFA SHUTDOWN COMPLETE is logged.

2. Stop CA Insight DPM data collectors by entering the following console command for each DB2 subsystem:

   P *db2ssid*DC

   db2ssid

   Identifies the DB2 subsystem ID.

   Message IEF404I ssidDB2 - ENDED - TIME=*hh:mm:ss* is logged.

3. Stop the CA Insight DPM program call owner:

   ```
   P IDB2PC
   ```

   Message IEF404I IDB2PC - ENDED - TIME=*hh:mm:ss* is logged.

4. Stop Xnet by entering the following console command:

   ```
   P PXNPROC
   ```

   Message IEF404I PXNPROC - ENDED - TIME=*hh:mm:ss* is logged.

5. Stop Xmanager:

   ```
   P PTXMAN
   ```

   Message IEF404I PTXMAN - ENDED - TIME=*hh:mm:ss* is logged.

Stop CA Chorus Infrastructure Management for Networks and Systems Components

Select the following procedures based on your configuration.

Stop the SYSVIEW Started Task

The Main Services Address Space can be terminated using the z/OS STOP (P) command. The task can be stopped from a system console by entering the command P SYSVIEW.

Stop CA NetMaster NM for TCP/IP Components

Use this procedure to stop CA NetMaster NM for TCP/IP components that provide data to CA Chorus Infrastructure Management for Networks and Systems:

Follow these steps:

1. Stop the SOLVE SSI region by issuing the following command from the MVS console:

   P *ssiname*

   ssiname

   Name you specified for the SOLVE SSI during the CA NetMaster NM for TCP/IP setup process.

2. Stop the product region:

   P *rname*

   rname

   Name you specified for the region during the CA NetMaster NM for TCP/IP setup process.

Stop CA Chorus for Security and Compliance Management Components

Select the following procedures based on your configuration.

Stop the CIA Real-Time Component

To stop the CIA real-time component address space, issue the following command at the console:

```
P CIARTUPD
```

Note: If you changed the name of the CIA real-time component procedure, specify that value in the command rather than CIARTUPD.

Stop the Router

You can stop the Router address space at any time.

To stop the Router component, issue the following command at the console:

```
P CMGRRTR
```

Note: CMGRRTR represents the active CA Compliance Manager procedure.

Important! Stopping the Router shuts down not only the Router but also any associated active component address spaces, including the following:

- Alert component (CMGRALRT started task procedure)
- Logger component (CMGRLOGR started task procedure)
- Monitor component (CMGRMON started task procedure)
- Warehouse component (CMGRWHSE started task procedure)

Stop the Alert Component

Use this procedure to stop the Alert component address space at any time.

To stop the Alert component, issue the following command at the console:

```
P CMGRALRT
```

Note: CMGRALRT represents the active CA Compliance Manager procedure.

Stop the Logger Component

Use this procedure to stop the Logger component address space at any time.

To stop the Logger component, issue the following command at the console:

```
P CMGRLOGR
```

Note: CMGRLOGR represents the active CA Compliance Manager procedure.

Stop the Warehouse Component

Use this procedure to stop the Warehouse component address space at any time.

To stop the Warehouse component, issue the following command at the console to shut down the Warehouse component address space:

```
P CMGRWHSE
```

Note: CMGRWHSE represents the active CA Compliance Manager procedure.

Stop the Monitor Component

You can stop the Monitor component address space at any time.

To stop the Monitor component, issue the following command at the console:

```
P CMGRMON
```

Note: CMGRMON represents the active CA Compliance Manager procedure.

Stop CA Chorus for Storage Management Components

To shut down the host server, use *one* of the following commands:

```
F SAMS,STOP
P SAMS
```

We recommend that you use the F SAMS,STOP command. Both commands cause an orderly shutdown in the same way. However, if you use the MODIFY command (F SAMS,STOP), z/OS does not terminate the console communication. Also, you can continue to issue the modify commands during the shutdown period. Console communication can be valuable when a component fails to shut down smoothly.

If you use the stop command (P SAMS), z/OS immediately terminates the console communication with the host server. If you then try to issue more modify commands, z/OS responds with the following message:

```
IEE342I MODIFY REJECTED-TASK BUSY
```

Modify the Session Timeout

Users are logged out of the system after 30 minutes by default. Use this procedure to modify the session timeout setting for all CA Chorus instances that are defined to a JBoss server. The CA Chorus administrator must perform this procedure.

Follow these steps:

1. Edit the ENVETJ member in *chorus_runtime_hlq*.CETJOPTN to change the following parameter value to the applicable number of minutes for the session timeout:

   ```
   # For JBoss session timeout configuration
   IJO="$IJO -Dchorus.jboss.session.timeout.minutes=45"
   ```

2. Stop the JBoss server:

   ```
   P CHORJBOS
   ```

   A message indicating that the JBoss server started task has ended is logged.

3. Start the JBoss server:

   ```
   S CHORJBOS
   ```

   A message indicating that startup is complete is logged, and the new session timeout value is in effect.

Customize Teiid Timeout Value

The Teiid timeout value to execute a query is 300 seconds by default. If a Teiid query execution exceeds the default value, Teiid stops the execution, and Teiid returns an error message. Use this procedure to set the Teiid timeout value in CA Chorus. The system administrator must perform this procedure to set the custom environment variable.

Note: To configure this setting such that Teiid never times out, use a negative value, such as -1.

Follow these steps:

1. Edit the ENVETJ member in *chorus_runtime_hlq*.CETJOPTN to set the session timeout in seconds:

   ```
   # For Teiid timeout configuration
    IJO="$IJO -Dcom.ca.chorus.queryTimeout=350"
   ```

2. Stop the JBoss server:

   ```
   P CHORJBOS
   ```

   A message indicating that the JBoss server started task has ended is logged.

3. Start the JBoss server:

   ```
   S CHORJBOS
   ```

   A message indicating that startup is complete is logged, and the new Teiid timeout value is in effect.

Disable Automatic Configuration of Heap Memory

CA Chorus automatically configures the heap memory size based on the disciplines that you install at JBoss startup. If you do not want CA Chorus to do so, disable the automatic configuration.

Follow these steps:

1. Edit the CHORJBOS member in *chorus_runtime_hlq*.CETJJCL to change the following parameter value to N (No):

   ```
   PARM='HEAPCNFG CALCULATE==N'
   ```

2. Start the JBoss server:

   ```
   S CHORJBOS
   ```

   Messages are logged indicating that the automatic configuration of heap memory is disabled and that startup is complete.

3. (Optional) If you are disabling automatic configuration after the initial CA Chorus configuration, copy the CHORJBOS member to a PROCLIB.

   The automatic configuration of heap memory is disabled.

Note: To modify the heap memory size, see the Java heap size (Java SDK Option) setting in the ENVETJ member of *chorus_runtime_hlq.*CETJOPTN. For the heap range, -Xms is the starting value, and -Xmx is the ending value.

Note: For information about heap memory size requirements, see the *Site Preparation Guide*.

Chapter 2: Managing High Availability

How to Implement HA Automatic Restart Management

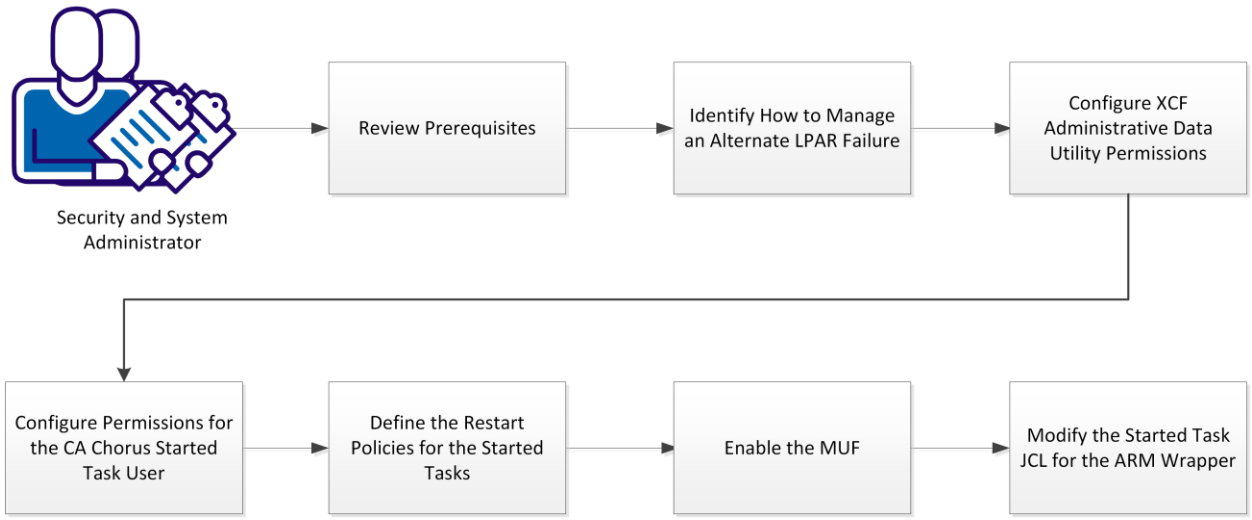
High Availability (HA) is a system design approach such that when a system fails, users can continue working on another system. For example, if the LPAR fails where CA Chorus is running, users need instant access to a secondary LPAR running the product.

This scenario explains how a system administrator and security administrator implement HA. Doing so can save time and money because users do not lose access in a single-fault scenario.

For CA Chorus HA, you configure the product to integrate with the z/OS Automatic Restart Management (ARM) facility. If a failure occurs, this facility provides the following HA options:

- Automatically restart an address space on the same system.
- Restart the address spaces on another system in a sysplex.

How to Configure CA Chorus with z/OS Automatic Restart Management



To implement the ARM facility, complete the followings steps:

1. Review Prerequisites. (see page 35)
2. Identify How to Manage an Alternate LPAR Failure. (see page 36)
3. Configure XCF Administrative Data Utility Permissions (see page 37).
4. Configure Permissions for the CA Chorus Started Task User. (see page 39)
5. Define the Restart Policies for the Started Tasks. (see page 41)
6. Enable the MUF. (see page 41)
7. Modify the Started Task JCL for the ARM Wrapper. (see page 42)

Review Prerequisites

Complete the following tasks before starting this scenario:

1. Review the z/OS sysplex and coupling facility feature of the z/OS operating system. We recommend that you understand this facility before attempting to configure it. The following IBM manuals provide detailed information regarding how to configure Automatic Restart Manager (ARM) in a z/OS environment:
   - *z/OS MVS Setting up a Sysplex*
   - *z/OS Communications Server IP Configuration Guide* for configuring VIPA to direct browser requests
   - *z/OS Distributed File Service zFS Administration Guide*
   - *z/OS MVS Sysplex Services Guide*
2. Set up XCF data sets on your z/OS systems. The details of this prerequisite are outside of the scope of this scenario. For more information, see ARM in *z/OS MVS Setting up a Sysplex.* IBM provides sample JCL streams in SYS1.SAMPLIB to format the XCF ARM data set (IXCARMF) and define policies (IXCARMP0).
3. Configure the failover LPAR to meet CA Chorus security requirements. Minimally, configure the following items for the failover LPAR:
   - CHORADM (run ETJI095*x*, where *x* indicates the security product (A for CA ACF2, T for CA Top Secret, and R for IBM RACF)
   - CA Chorus resource class
   - Passtickets

   More changes vary based on the existing configuration of the failover LPAR.

Note: For a detailed list of all security requirements, see the *Site Preparation Guide*.

Identify How to Manage an Alternate LPAR Failure

Use this topic to determine your plan for failing to an alternate LPAR.

Consider the following scenarios:

1. If you use the Knowledge Center to index content only available on the LPAR where CA Chorus is running, this content is not available when the product switches to a different LPAR. Switching can occur when you have configured the product for High Availability (HA). After the product reverts to the LPAR where the content resides, the content is available.
2. Determine your LPAR configuration:
   - When an address space fails on a healthy LPAR, ARM automatically restarts the address space on the LPAR where it failed.
   - If ARM is configured for a sysplex environment with more than one LPAR and the LPAR where CA Chorus is running fails, ARM can automatically restart all started tasks in order on an alternate LPAR in the same sysplex. To accomplish this goal for the CA Chorus JBoss server, mount the product zFS file systems on the alternate LPAR before JBoss can start. Review and identify the best option for this configuration:

     Important! To the mount the zFS file system, CHORADM requires an OMVS segment with READ access to BPX.SUPERUSER. For example, IBMFAC(BPX.SUPERUSER) ACCESS(READ).

     - Create a set of mirror file systems on the alternate LPAR for read/write.

       Of the file systems that are created during product installation, only CETJZFS0, CETJLOGS, and CETJDB are required to be mounted as read/write. All other file systems can be mounted read-only on both LPARs. You can then create alternate copies of the three read/write file systems so that each LPAR has its own copy of the file systems. You would then need to periodically synchronize the CETJDB file system between the systems. The disadvantage to this configuration is that the CETJDB file system does not contain updates that CA Chorus has made on the primary LPAR since the last synchronization.
     - Mount the file systems on both LPARs using zFS sysplex-aware file systems.

       Starting with z/OS v1.11, you can run zFS as sysplex-aware. The read/write file systems can be mounted simultaneously on the primary and alternate LPARs.
     - Add a step to CHORJBOS on the alternate LPAR to mount the file systems before the JBoss step.

Because the JBoss server only starts on the alternate LPAR when the primary LPAR fails, do not mount the file systems in another location when the alternate JBoss server starts. If a step is added to the CHORJBOS started task to execute MOUNT commands for the necessary file systems, the CHORJBOS on the alternate LPAR continues using the data from the primary LPAR. This setup means that you cannot restart the JBoss server on the primary LPAR until you shut down the server on the alternate LPAR. You must also unmount the file systems.

Note: If you choose this option, implement it during Modify the Started Task JCL for the ARM Wrapper (see page 42).

So, a situation cannot arise where the server is running simultaneously on two different LPARs. This situation could occur with the other options.

Configure XCF Administrative Data Utility Permissions

The IBM utility IXCMIAPU lets you add, update, delete, and list policy data on the Automatic Restart Management (ARM) couple data set. Use of this utility is restricted using a resource named MVSADMIN.XCF.ARM in the IBMFAC resource class. The ARM user must have UPDATE access to add, update, and delete policy data. The ARM user must also have READ access to produce reports.

This user is only used to update the z/OS ARM policy, which you need only perform once. The ARM user is not a CA Chorus user.

Sample: Use CA ACF2 to Configure XCF Administrative Data Utility Permissions

This example shows how to use CA ACF2 commands to configure access to this utility.

For detailed information about these commands, see the CA ACF2 documentation.

Follow these steps:

1. Give the ARM user access to the ARM resource:

   ```
   SET RES(FAC)
   RECKEY MVSADMIN ADD(XCF.ARM) UID(uid_of_ARM_user) SERVICE(READ,UPDATE) ALLOW)
   ```

2. Activate your changes:

   ```
   F ACF2,REBUILD(FAC),C(R)
   ```

   The permissions are set.

Sample: Use CA Top Secret to Configure XCF Administrative Data Utility Permissions

This example shows how to use CA Top Secret commands to configure access to this utility.

For detailed information about these commands, see the CA Top Secret documentation.

Follow these steps:

Note: The first step applies only if the resource is not owned.

1. Add the ARM resource to the appropriate ACID:

   ```
   TSS ADDTO(ACID) IBMFAC(MVSADMIN.XCF.ARM)
   ```

2. Give the ARM user access to the ARM resource:

   ```
   TSS PERMIT(ARM_user) IBMFAC(MVSADMIN.XCF.ARM) ACCESS(READ,UPDATE)
   ```

   The permissions are set.

Sample: Use IBM RACF to Configure XCF Administrative Data Utility Permissions

This example shows how to use IBM RACF commands to configure access to this utility.

For detailed information about these commands, see the IBM RACF documentation.

Follow these steps:

1. Activate the facility class:

   ```
   SETROPTS CLASSACT(FACILITY)
   ```

2. Define the ARM resource to the ARM facility:
   ```
   RDEFINE FACILITY MVSADMIN.XCF.ARM UACC(NONE)
   ```

3. Give the ARM user access to the ARM facility:

   ```
   PERMIT MVSADMIN.XCF.ARM CLASS(FACILITY) ID(ARM_user) ACCESS(READ,UPDATE)
   ```

4. Activate your changes:

   ```
   SETROPTS RACLIST(FACILITY) REFRESH
   ```

   The permissions are set.

Configure Permissions for the CA Chorus Started Task User

The user name that is associated with the CA Chorus started tasks requires permissions to register and deregister with ARM at initialization and termination of the various components. The following values apply regardless of which security system that you use to configure permissions:

stc-userid

Indicates the default user name that is associated with the CA Chorus started tasks in ETJI095*x* in *chorus_runtime_hlq*.CETJJCL.

Default: CHORADM

IXCARM

Identifies the z/OS Automatic Restart Manager.

Sample: Use CA ACF2 to Configure CA Chorus Started Task User Permissions

This example shows how to use CA ACF2 commands to configure the started task user permissions.

For detailed information about using these commands, see the CA ACF2 documentation.

Follow these steps:

1. Give the STC ID access to the ARM facility:

   ```
   SET RESOURCE(FAC)
   RECKEY IXCARM ADD(- UID(stc-userid) SERVICE(READ,UPDATE) ALLOW
   ```

2. Activate your changes:

   ```
   F ACF2,REBUILD(FAC),C(R)
   ```

   The started task can use ARM.

Sample: Use CA Top Secret to Configure CA Chorus Started Task User Permissions

This example shows how to use CA Top Secret commands to configure the started task user permissions.

For detailed information about using these commands, see the CA Top Secret documentation.

Follow these steps:

Note: The first step applies only if the resource is not owned.

1. Add the ARM resource to the appropriate ACID:

   `TSS ADDTO(ACID) IBMFAC(IXCARM)`

2. Give the STC ACID access to the ARM resource:

   `TSS PERMIT(stc-acid) IBMFAC(IXCARM.) ACCESS(READ,UPDATE)`

   The started task can use ARM.

Sample: Use IBM RACF to Configure CA Chorus Started Task User Permissions

This example shows how to use IBM RACF commands to configure the started task user permissions.

For detailed information about these commands, see the IBM RACF documentation.

Follow these steps:

1. Activate the facility:

   `SETROPTS GENERIC(FACILITY)`

2. Define the ARM resource to the ARM facility:

   `RDEFINE FACILITY IXCARM.* UACC(NONE)`

3. Give the STC ID access to this facility:
   `PERMIT IXCARM.* CLASS(FACILITY) ID(stc-userid) ACCESS(READ,UPDATE)`

4. Activate your changes:

   `SETROPTS RACLIST(FACILITY) REFRESH`

   The started task can use ARM.

Define the Restart Policies for the Started Tasks

The ETJARMP member in the *chorus_runtime_hlq*.CETJJCL data set provides a sample job stream. Use this member to define an ARM policy for the CA Chorus started tasks.

Follow these steps:

1. Customize this member to conform to your environment. Follow the instructions that are included in the comments.
2. Execute the following z/OS console command to apply your changes:

   ```
   SETXCF START,POLICY,TYPE=ARM,POLNAME=CHORPOL1
   ```

   The restart policies are defined.

Enable the MUF

CA Datacom/AD includes built-in support for Automatic Restart Management (ARM). You must enable this support for High Availability.

Note: If ARM is not enabled, you can rerun Automatic Configuration or can edit the jobs manually, as noted in this procedure. For Automatic Configuration details, see the *Installation Guide*.

Follow these steps:

1. Confirm that the CPYAXDAT job was run from *chorus_runtime_hlq*.CETJJCL to copy the sample AXDATIN1 and AXDATIN2 members from *chorus_runtime_hlq*.CETJOPTN to *datacomad_adchlq*.CUSMAC.
2. Edit the Multi-User Facility (MUF) control options file in AXDATIN1, which resides in *datacomad_adchlq*.CUSMAC:
   a. Uncomment the ARM option, which is the first line in OPTIONAL START-UP PARMS FOR AXDATIN1.
   b. Ensure that the element name corresponds to an element name that is defined in the ARM policy. The default is CHORMUF.
3. Restart the CA Datacom/AD database MUF:

   ```
   S your_muf_name
   ```

   The following messages appear:

   - Message DB00212I appears on the z/OS console to identify the release of CA Datacom/AD that you have installed.
   - Message DB00201I appears on the z/OS console to indicate that the MUF is up.

   Important! Confirm that the MUF started before you continue.

Modify the Started Task JCL for the ARM Wrapper

The CHRARMW utility is used for registering and deregistering the CA Chorus started tasks with the Automatic Restart Manager (ARM).

Members of *chorus_runtime_hlq*.CETJJCL contain commented steps to complete the following tasks:

- Register the started task with ARM before the main step execution (ARMREG).
- Deregister the started task with ARM after the main step has successfully terminated (ARMDEREG).

ARM uses the following process to determine whether to restart a started task:

- If the main step terminates with a non-zero condition code or abends, the ARMDEREG step does not execute.
- If either option occurs, ARM automatically restarts the started task after address space termination.
- The registration step specifies an element name. The default is the job name. Ensure that the element name corresponds to an element name in the ARM policy that was created in the previous step.

Note: If ARM is not enabled, you can rerun Automatic Configuration or can edit the jobs manually, as noted in this procedure. For Automatic Configuration details, see the *Installation Guide*.

Follow these steps:

1. Edit the ARM parameters in the CHORJBOS, CHORTSF, and CHORTSFR members in *chorus_runtime_hlq*.CETJJCL as described in the member and save your changes.

   The started task JCL is updated.

2. Copy the CHORJBOS and CHORTSF PROC into a specific PROCLIB for each eligible system. Edit both copies of CHORJBOS to match the configuration of the system.

   Note: If a TSF Engine (CHORTSF) is copied to an LPAR where a TSF relay (CHORTSFR) runs, stop the TSF relay to let the engine run.

3. If the failover system has different system values for the values in the ENV* members that are located in CETJOPTN, copy the ENV* members and reference them from the PROCLIB of each system.

4. If you have TSF relays on other LPARs, update their CETJOPTN(TSFRPRMS) member to point to the new TTSFHOST.

5. Restart the CHORTSF started task by entering the following console command:

   ```
   S CHORTSF
   ```

   When TSF is available, the following message appears on the z/OS console:

   N00503 *** TSF INITIALIZATION COMPLETE TSF ***

6. Restart the CHORTSFR started task on your remote LPARs, if applicable:

   ```
   S CHORTSFR
   ```

   A message indicating that TSFR initialized is logged.

7. Restart the CHORJBOS started task:

   ```
   S CHORJBOS
   ```

   The following message appears when JBoss startup is complete:

   ```
   ETJTC001I CA Chorus Startup Complete
   ```

You have successfully configured High Availability for CA Chorus using z/OS Automatic Restart Management.

Chapter 3: Managing Databases

Stop CA Datacom/AD Database MUF

You can stop the CA Datacom/AD database Multi-User Facility (MUF) to run cleanup jobs and as needed.

Stop the CA Datacom/AD database MUF:

P *your_muf_name*

The CA Datacom/AD database MUF is stopped.

Reinitialize the CA Chorus Database

The CA Chorus database initialization can be restarted at any time. Your MUF must be active when you start this procedure.

Important! Upon completion of this procedure, saved database data is erased.

Follow these steps:

1. Follow site requirements to delete databases (user notification, management approval, and so on).
2. Submit CHDB101 in *chorus_runtime_hlq*.CETJJCL to remove the database definition from the CA Datacom/AD MUF for CA Chorus.
3. Submit CHDB102 in *chorus_runtime_hlq*.CETJJCL to delete the CA Chorus database data sets.
4. Submit CHDB004 in *chorus_runtime_hlq*.CETJJCL to recreate the database.

   The CA Chorus database is initialized.

Reinitialize the Time Series Facility Database

The Time Series Facility (TSF) database initialization can be restarted at any time. Your MUF must be active when you start this procedure.

Important! Upon completion of this procedure, saved TSF database data is erased.

Follow these steps:

1. Follow site requirements to delete databases (user notification, management approval, and so on).
2. Submit TSDB102 in *chorus_runtime_hlq*.CETJJCL to remove the database definition from the CA Datacom/AD MUF for CA Chorus.
3. Submit CHTSDBDL in *chorus_runtime_hlq.*CETJJCL to delete the CA Chorus database data sets.
4. Submit TSDB002 in *chorus_runtime_hlq.*CETJJCL to recreate the database.

   The TSF database is initialized.

Time Series Facility Database

The Time Series Facility (TSF) provides a single point for collection, storage, management, and organization of product data. The TSF database stores data collected and provided by the following products:

- CA Detector for DB2 for z/OS supplies data for CA Chorus for DB2 Database Management.
- CA SYSVIEW and CA NetMaster NM for TCP/IP supply data for CA Chorus Infrastructure Management for Networks and Systems.
- CA ACF2 for z/OS or CA Top Secret for z/OS supplies data for CA Chorus for Security and Compliance Management.
- CA Vantage SRM supplies data for CA Chorus for Storage Management.

When you request a Time Series chart in the Investigator, CA Chorus displays the data stored in the TSF database. The Investigator helps you view and analyze information stored in role-specific data repositories by providing multiple work areas (panes) to help you manage your data.

The space requirements for the Time Series Facility (TSF) database are a function of the selected TSF parameters. Additionally, the space requirements are a function of the amount of activity on the systems being monitored. The TSF database consists of the following areas:

Note: All but G014003 use the JCL parm DSNTYPE=LARGE, which lets a data set be over 65,535 tracks.

G01

Contains the product registration information.

G02

Contains the entity key values for the data points stored in G03.

G03

Contains the actual data points.

G04

Contains the actual data points.

IXX

Contains the CA Datacom/AD key information for all data areas in the TSF database.

The IXX area has Auto Dynamic Extend enabled by default. Areas G01/2/3/4 have Auto Dynamic Extend enabled by default.

Note: Multivolume INITs: You can initialize these areas across multiple extents on multiple volumes. For a description about how the operating system handles secondary allocations, see your operating system JCL manual.

TSF Database Recommendations

Given that each site and configuration can vary significantly, use the following examples as a general reference as you plan your TSF database sizing activities. Each example includes the key variables to consider when sizing the database for your CA Chorus discipline.

These examples assume that you are using default settings for metrics management. If you lengthen the retention period, the database should be larger and vice versa. For more details, see metrics management settings (see page 59).

As you review each example, consider the following points:

- G04 receives all data feeds.
- Data moves from the G04 area to the larger G03 area on an hourly basis.
- Metrics management runs nightly to manage G03.

In general, G04 is about half the size of G03. To retain data longer using Metric Management parameters, increase the size of G03. To capture more data (for example, from many LPARs), increase the size of G03 *and* G04.

CA Chorus for DB2 Database Management TSF Database Recommendations

This example uses the following CA Chorus for DB2 Database Management default metric management parameters:

- MMT1EXPIRY = 1D = 1 day
- MMT2EXPIRY = 3M = 3 Months

The following estimates are based on a given model size for a DB2 subsystem. Consider the size of each DB2 subsystem in your environment and total these together to arrive at the recommended cylinder requirement.

DB2 Subsystem Size	Number of Unique Plans	Number of Unique Packages per Plan	Recommended Cylinders
Small	1	5	121
Medium	1	10	482
Large	1	20	1928
Extra Large	1	30	4338

Example Environment

DB2 Subsystem Size	Number of DB2 Subsystems	Recommended Cylinders Per DB2 Subsystem Size
Medium	2	964
Large	3	5784
Extra Large	1	4338

Total Recommended Cylinders: 11086

CA Chorus Infrastructure Management for Networks and Systems TSF Database Recommendations

CICS

This example uses the following Infrastructure Management default metric management parameters:

- MMT1EXPIRY = 7D = 7 days
- MMT2EXPIRY = 8D = 8 days

Given the following Infrastructure Management CICS TSF feeds:

Total CICS Regions Feeding TSF	Total CICS Transactions (per CICS)	Recommended TSF Database Cylinders (G03 Area)
10	25	905
	40	1421
	50	1764
25	25	2262
	40	3551
	50	4410
50	25	4523
	40	7100
	50	8818

IMS

This example uses the following Infrastructure Management default metric management parameters:

- MMT1EXPIRY = 7D = 7 days
- MMT2EXPIRY = 8D = 8 days

Given the following Infrastructure Management IMS TSF feeds:

Total IMS Subsystems	Total IMS Transactions (per IMS)	Total IMS buffer pools (per IMS)	Total IMS pools (per IMS)	Recommended TSF Database Cylinders (G03 Area)
10	25	20	150	1450
	40	20	150	1815

Total IMS Subsystems	Total IMS Transactions (per IMS)	Total IMS buffer pools (per IMS)	Total IMS pools (per IMS)	Recommended TSF Database Cylinders (G03 Area)
	50	20	150	2059
25	25	20	150	3623
	40	20	150	4537
	50	20	150	5147
50	25	20	150	7244
	40	20	150	9073
	50	20	150	10293

CA NetMaster NM for TCP/IP

This example uses the following Infrastructure Management default metric management parameters:

- MMT1EXPIRY = 7D = 7 days
- MMT2EXPIRY = 8D = 8 days

The database size calculations for the other Infrastructure Management components adequately support the data provided by the NetMaster TSF feeds.

MVS

This example uses the following Infrastructure Management default metric management parameters:

- MMT1EXPIRY = 7D = 7 days
- MMT2EXPIRY = 8D = 8 days

This example also assumes that the default CA SYSVIEW TSF feed configuration where channel and device feeds are turned off.

Given the following Infrastructure Management MVS TSF feeds:

Total LPARs Feeding TSF	Total TSF-Monitored Jobs (per LPAR)	Recommended TSF Database Cylinders (G03 Area)
10	50	1109
	100	2162
	150	3215

Total LPARs Feeding TSF	Total TSF-Monitored Jobs (per LPAR)	Recommended TSF Database Cylinders (G03 Area)
25	50	2772
	100	5404
	150	8037
50	50	5543
	100	10808
	150	16073

If TSF device monitoring is turned on, add the following space recommendations to the initial MVS recommendation:

Total LPARs Feeding TSF	Total TSF-Monitored Jobs (per LPAR)	Recommended TSF Database Cylinders (G03 Area)
10	50	111
	100	222
	150	333
25	50	278
	100	555
	150	832
50	50	555
	100	1109
	150	1663

If TSF channel monitoring is turned on, add the following space recommendations to the initial MVS recommendation:

Total LPARs Feeding TSF	Total TSF-Monitored Jobs (per LPAR)	Recommended TSF Database Cylinders (G03 Area)
10	256	568
25	256	1419
50	256	2838

WEBMQ

This example uses the following Infrastructure Management default metric management parameters:

- MMT1EXPIRY = 7D = 7 days
- MMT2EXPIRY = 8D = 8 days

Given the following Infrastructure Management WEBMQ TSF feeds:

Total WEBMQ qmgrs	Total WEBMQ Channels	Total WEBMQ Queues	Recommended TSF Database Cylinders (G03 Area)
5	100	100	672
		500	1780
	500	100	1337
		500	2446
15	100	100	2014
		500	5340
	500	100	4010
		500	7335
30	100	100	4028
		500	10679
	500	100	8018
		500	14669

CA Chorus for Security and Compliance Management TSF Database Recommendations

The following chart uses the following TSFPARMS (member of CETJOPTN) metric management tier parameters:

- MMT1EXPIRY = 1D = 1 day
- MMT2EXPIRY = 14D = 14 days

The following chart is based on the statistics interval value taken from the security products parameter: CHORUSSTATI

If your security product collects statistical data for Command Propagation Facility (CPF) nodes, this chart also provides recommended values for up to five CPF nodes.

Number of Systems (LPARS)	Security Chorus Statistics Interval Value	Recommended TSF Database Cylinders for System	Recommended TSF Database Cylinders for CPF nodes	Recommended TSF Database Cylinders Total
1	30 seconds	5	1	6
	60 seconds	4	1	5
	15 minutes	3	1	4
	30 minutes	3	1	4
3	30 seconds	15	3	18
	60 seconds	8	2	10
	15 minutes	7	1	8
	30 minutes	7	1	8
5	30 seconds	24	5	29
	60 seconds	16	4	20
	15 minutes	11	2	13
	30 minutes	11	1	12

The following chart uses the following TSFPARMS (member of CETJOPTN) metric management tier parameters:

- MMT1EXPIRY = 7D = 7 days
- MMT2EXPIRY = 8D = 8 days

The chart is based on the statistics interval value taken from the security products parameter: CHORUSSTATI

If your security product collects statistical data for Command Propagation Facility (CPF) nodes, this chart also provides recommended values for up to five CPF nodes.

Number of Systems (LPARS)	Security Chorus Statistics Interval Value	Recommended TSF Database Cylinders for System	Recommended TSF Database Cylinders for CPF nodes	Recommended TSF Database Cylinders Total
1	30 seconds	23	6	29
	60 seconds	13	3	16
	15 minutes	3	1	4
	30 minutes	3	1	3
3	30 seconds	69	16	85
	60 seconds	38	9	47
	15 minutes	8	2	10
	30 minutes	7	1	8
5	30 seconds	115	27	142
	60 seconds	63	15	78
	15 minutes	14	3	17
	30 minutes	11	2	13

CA Chorus for Storage Management TSF Database Recommendations

Using the following storage discipline objects and Intervals Per Day examples, we recommend 7,957,846 KB (approximately 141 cylinders) for your TSF database. Review your PERFOM_EVT_PROC=INTERVAL= statement in each CA Vantage SRM logging script to determine how many Intervals Per Day are occurring and the cylinders required for growth.

For the Storage Management TSF parameters, this tier is set where MMT1EXPIRY = 14D = 14 days.

Object	Description	Intervals Per Day	Record Length in Bytes	Number of Records
LPACEPO	Online DASD Volume Statistics	28	110	1000
POOLS	Storage Groups	12	075	100
CATALOGJ	Catalogs Statistics	04	132	003
OBJ02410	Catalogs I/O Statistics	48	100	300
OBJ02408	Catalog Cache Statistics	48	082	300
GRPCBS	Application Data Sets Statistics	02	114	129

Increase Data Set Space Allocations

System administrators can add space to the TSF database after customizing the database to optimize database space performance and to reclaim free space. Adding more space enables continuous use of the database when the data area is full.

You can add space to the TSF database by increasing data set space allocations. A backup, delete, define, and reload of the database is performed through JCL. Use this option to control the number of extents used. A backup and load is required if you want to retain the data.

Note: Sample JCL is provided in *chorus_runtime_hlq*.CETJJCL. You can run the CHTSDBBK periodically to create a backup of the database.

Follow these steps:

1. Confirm that your CA Datacom/AD MUF for CA Chorus is active.
2. Edit the following members located in *chorus_runtime_hlq*.CETJJCL as described in the members:

   CHTSDBBK

   Creates a backup of the TSF database.

   TSDB102

   Deletes the TSF database definition in the CA Datacom/AD MUF.

   CHTSDBDL

   Deletes the existing TSF database files.

   TSDB002

   Allocates and defines the TSF database to the CA Datacom/AD MUF. Change the space allocations for IXX4003, G014003, G024003, G034003, and G044003 in accordance with the increased space requirement.

   Note: TSDB002 allocates the files needed for the TSF database and performs an initial load, which creates a database with schema definitions but no data.

   CHTSDBLD

   Loads the TSF database from the backup.

3. Reallocate the TSF database by executing the following steps in the order shown:

   Important! Select a time to run these jobs that least impacts your users.

   a. Stop the CHORJBOS and CHORTSF started tasks:

      ```
      P CH0RJB0S
      P CH0RTSF
      ```

   b. Submit CHTSDBBK.

      A backup version of the database is created.

   c. Submit TSDB102.

      TSF database definition is deleted from the CA Datacom/AD MUF.

   d. Submit CHTSDBDL.

      The TSF database files are deleted.

   e. Submit TSDB002 (includes adjusted space requirements from step 2).

      The TSF database is created.

f. Submit CHTSDBLD.

The TSF database is loaded from the backup made in CHTSDBBK.

g. Start the CHORTSF and CHORJBOS started tasks:

```
S CHORTSF
S CHORJBOS
```

The TSF database is reallocated.

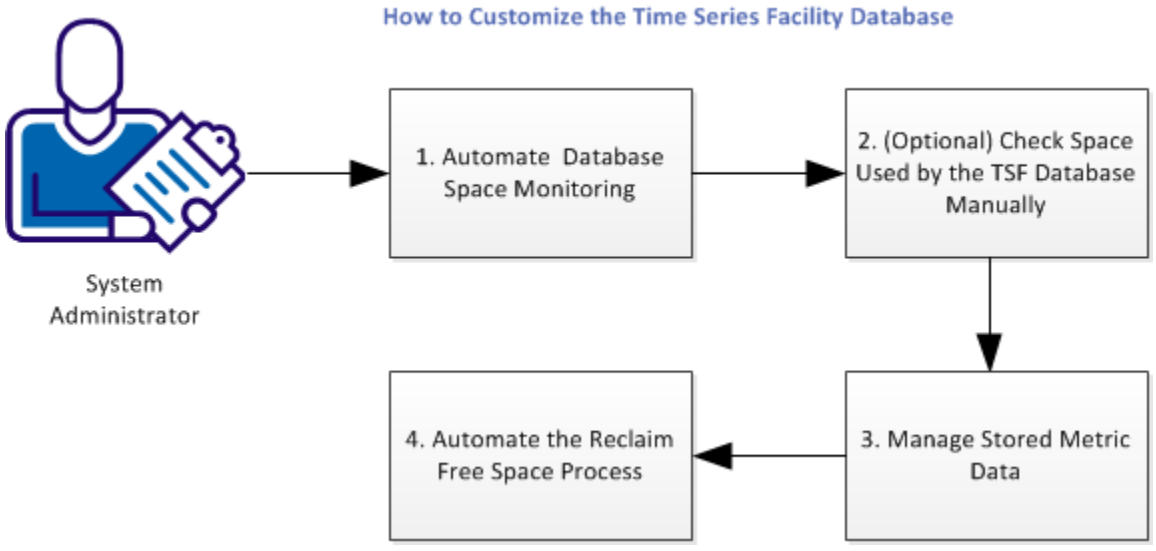
Note: A return code of 0 is expected from all jobs.

You have successfully increased the data set space allocations and helped ensure continuous operation of the database.

How to Customize the Time Series Facility Database

The Time Series Facility (TSF) provides a single point for collection, storage, management, and organization of product data. When you request a Time Series chart in the Investigator, CA Chorus displays the data stored in the TSF database. The Investigator helps you view and analyze information stored in role-specific data repositories by providing multiple work areas (panes) to help you manage your data.

This scenario shows how a system administrator can customize the TSF database to optimize its performance. The following illustration describes the tasks to customize the TSF database:



Note: For the first and fourth tasks, you identify CA Chorus messages and then define them as triggers in your automation product, such as CA OPS/MVS.

Perform the following tasks to customize the TSF Database:

1. Automate Database Space Monitoring (see page 58)
2. (Optional) Check Space Used by the TSF Database Manually (see page 59)
3. Manage Stored Metric Data (see page 59)
4. Automate the Reclaim Free Space Process (see page 65)

Automate Database Space Monitoring

TSF provides a database space use monitor. This monitor runs once per hour on the half hour to measure the number of blocks used for the data area and system area. The number of blocks used includes all blocks that contain any data, from nearly empty to 100 percent full. When the usage of a data block or a system block moves above 80 percent, the monitor issues warning message ETJTS454W. The accompanying informational messages ETJTS455I and ETJTS456I provide details about the current use of each data and system area.

Whenever a data area reaches 100 percent block use, you must take the database offline. The dynamic extend facility automatically extends the data area when it becomes full and lets you continue with the database. Space is added as an additional extent using the secondary allocation amount defined for the data set in the TSDB002 job.

Dynamic extend provides temporary relief from a full condition. Schedule a manual increase in the size of the database as soon as possible. Without a manual increase in database size, the dynamic extend feature repeats each time the data area reaches 100 percent block use. This cycle continues until an IEC030I B37-04 message condition occurs.

Follow these steps:

1. Launch your automation product, such as CA OPS/MVS.
2. Define ETJTS454W as a trigger or event message to generate a notification that the space use is high and you must increase the TSF database space allocation. Complete this step using your site-specific practices.

   Database space monitoring is automated. When a threshold is exceeded, the ETJTS454W, ETJTS455I, and ETJTS456I messages appear.
3. Define the CA Datacom/AD message DB01705I as a trigger or event message to your automation tool. Doing so generates a notification message that a dynamic extend has started and that a user should manually schedule an increase in the size of the database. Complete this step using your site-specific practices.

(Optional) Check Space Used by the TSF Database Manually

The database space use monitor measures the block usage for each data area (G01, G02, and G03) and each system area (IXX and CXX). When the block usage for data area or system area goes over 80%, the command issues a warning message ETJTS454W.

You can manually check the space used by the TSF database by modifying CHTSDBRP in CETJJCL. Follow the steps in the member and submit the job.

Member CHTSDBRP is updated and the job is generated. The CHTSDBRP output shows the amount of space available and used for each area in the TSF database.

When the block usage for any area is nearing 100 percent, add space to the TSF database. Additionally, review the TSF metric management parameters to reduce the amount of stored data.

Manage Stored Metric Data

TSFPARMS member parameters in CETJOPTN let you control and reduce the amount of data being stored for all metrics that TSF collects. If you monitor multiple subsystems or you use multiple data feeds, you can alter the metric management parameters to minimize the amount of stored data. Alternatively, use these parameters to increase the TSF data storage capacity by using larger TSF data tables in the CA Chorus database MUF.

CA Chorus ships with default settings. After initial usage, we recommend that you review the defaults and adjust accordingly.

The TSF database is tiered so that data becomes less granular the longer it is stored. Records enter the TSF database at tier one, and roll into tier two and three as they reach their expiration age. If tier three is not specified, the records are deleted from the database. TSFPARMS member parameters in CETJOPTN let you control the expiration age of each tier.

The tier parameters are divided into the following groups so that the metrics can be processed differently:

Note: CA SYSVIEW and NETPERF parameters apply to CA Chorus Infrastructure Management for Networks and Systems.

Global

Applies to all metric sources.

Detector

Identifies a group of CA Chorus for DB2 Database Management-specific values that differ from the global settings. If set, these values override the global tier parameters.

NETPERF

Identifies a group of CA NetMaster NM for TCP/IP-specific values that differ from the global settings. If set, these values override the global tier parameters.

Security

Identifies a group of CA Chorus for Security and Compliance Management-specific values that differ from the global settings. If set, these values override the global tier parameters.

Storage

Identifies a group of CA Chorus for Storage Management-specific values that differ from the global settings. If set, these values override the global tier parameters.

SYSVIEW_CICS

Identifies a group of CA SYSVIEW-specific values for Customer Information Control System (CICS) Transaction Server that differ from the global settings. If set, these values override the global tier parameters.

SYSVIEW_IMS

Identifies a group of CA SYSVIEW-specific IMS values that differ from the global settings. If set, these values override the global tier parameters.

SYSVIEW_MVS

Identifies a group of CA SYSVIEW-specific values (z/OS, JES2, JES3) that differ from the global settings. If set, these values override the global tier parameters.

SYSVIEW_WEBMQ

Identifies a group of CA SYSVIEW-specific values (Websphere MQ) that differ from the global settings. If set, these values override the global tier parameters.

Follow these steps:

1. Open the TSFPARMS member of CETJOPTN and edit the global group to define the metric management tier parameters:
   a. Review and customize the following global tier parameters:

      MMT1EXPIRY=*nn*[D|W|M|Y]

      Specifies the expiration age for tier one in number of days, weeks, months, or years. Records that reach their tier one expiration age roll into tier two. No resolution is specified for tier one. Records enter the TSF database at this tier. The agent providing the data sets the resolution.

      Default: 14D (Global, Detector, Storage), 1D (Security) and 7D (NETPERF and all CA SYSVIEW options).

MMT2RESOLUTION=*nn*[M|H]

Specifies the time resolution for tier two samples in hours or minutes. Tier two records contain samples with a resolution equal to this value.

Values: M (minutes): 1, 5, 15, 30, or 60. H (hours): 1, 2, 4, 12, or 24

Default: 4H (Global, Detector, Storage), 30M (Security), and 1H (NETPERF and all CA SYSVIEW options).

Note: Tier resolution times must increase in size from one tier to the next.

MMT2EXPIRY=*nn*[D|W|M|Y]

Specifies the expiration age for tier two in number of days, weeks, months, or years. Records that reach their tier two expiration age roll into tier three. If tier three is not specified, the records are deleted from the TSF database.

Default: 3M (Global, Detector, Storage), 14D (Security), 8D (NETPERF) and 7D (all CA SYSVIEW options).

Note: Tier expiration ages must increase in age from one tier to the next. The age of the last tier is used to expire records from the TSF database, regardless of the tier where the records reside.

The default expiration age and resolution for the metric records are defined. To override these values, specify Detector, Infrastructure Management, Security, or Storage parameters.

b. (Optional) If you need more than two tiers, duplicate the MMT2EXPIRY and MMT2RESOLUTION parameters and customize them as MMT3EXPIRY and MMT3RESOLUTION. You can define up to five tiers, and they must be contiguous.

Note: Security includes MMT3 settings by default (MMT3RESOLUTION=4H and MMT3EXPIRY=3M).

2. Review and customize the discipline-specific tier parameters noted in Step 1a to define the following information:
   - Default expiration ages and resolution for the metric records.
   - Multiple tiers.

3. Identify when metric management starts by editing the following parameter:

   MMSTARTTIME=*hhmm*

   Specifies the preferred time in hours (*hh*) and minutes (*mm*) to start the daily metric management execution.

   Range: 0000 (midnight) to 2359

   Default: 0200

   The metric management start parameter is updated.

   Note: You can also start metric management on demand through the following console command: F CHORTSF,TSFMETMAN

4. Update the maximum metric management runtime by editing the following parameter:

   MMMAXRUNTIME=*hhmm*

   Specifies the maximum runtime of one metric management in hours (*hh*) and minutes (*mm*). With MMSTARTTIME, this parameter effectively limits the time frame that the metric management runs.

   Range: 0000 to 2400

   Default: 0400

   The metric management runtime is updated.

   TSFPARMS is updated and the metric management parameters are customized to control stored metric data.

Note: After each metric management execution, we recommend that you reclaim free space using the CHTSDBMT member of CETJJCL.

For more information about automating the free space reclaiming, see Automate the Reclaim Free Space Process (see page 65).

Example 1: Metric Management Sample Tiers Defined

```
MMSTARTTIME=0200
MMMAXRUNTIME=0400
*
<GLOBAL>
MMT1EXPIRY=14D
MMT2RESOLUTION=4H
MMT2EXPIRY=3M
*
<DETECTOR>
MMT1EXPIRY=14D
MMT2RESOLUTION=4H
MMT2EXPIRY=3M
* Tier 1 contains hourly data for 14 days. Tier 2 contains 4 hours of data and expires
after 3 months.
<SECURITY>
MMT1EXPIRY=1D
MMT2RESOLUTION=30M
MMT2EXPIRY=14D
MMT3RESOLUTION=4H
MMT3EXPIRY=3M
* Tier 1 contains hourly data for 1 day. Tier 2 contains 30 minutes of data and expires
after 14 days. Tier 3 contains 4 hours of data and expires after 3 months.
```

Example 2: Metric Management: All Tier Parameters

In this example, the Detector tier parameters are set to a longer time with two tiers. The Security tier parameters are set to a shorter time with four tiers. Global, Storage, SYSVIEW and NETPERF tier parameters are set to default values:

```
<GLOBAL>
MMT1EXPIRY=14D
MMT2RESOLUTION=4H
MMT2EXPIRY=3M

<DETECTOR>
MMT1EXPIRY=1M
MMT2RESOLUTION=12H
MMT2EXPIRY=4M

<SECURITY>
MMT1EXPIRY=1D
MMT2RESOLUTION=5M
MMT2EXPIRY=7D
MMT3RESOLUTION=30M
MMT3EXPIRY=1M
MMT4RESOLUTION=4H
MMT4EXPIRY=3M

<STORAGE>
MMT1EXPIRY=14D
MMT2RESOLUTION=4H
MMT2EXPIRY=3M

<SYSVIEW_CICS>
MMT1EXPIRY=7D
MMT2RESOLUTION=1H
MMT2EXPIRY=8D

<SYSVIEW_IMS>
MMT1EXPIRY=7D
MMT2RESOLUTION=1H
MMT2EXPIRY=8D

<SYSVIEW_MVS>
MMT1EXPIRY=7D
MMT2RESOLUTION=1H
MMT2EXPIRY=8D

<SYSVIEW_WEBMQ>
MMT1EXPIRY=7D
MMT2RESOLUTION=1H
MMT2EXPIRY=8D
```

```
<NETPERF>
MMT1EXPIRY=7D
MMT2RESOLUTION=1H
MMT2EXPIRY=8D
```

More information

Increase Data Set Space Allocations (see page 55)
TSF Database Recommendations (see page 47)

Automate the Reclaim Free Space Process

The TSF metric database uses large amounts of disk space. When a record is deleted from the TSF database, the space it occupied is reused for the new records. In some instances, the space is never reused if reclaiming is not done. To reclaim free space, we recommend that you run the CHTSDBMT member JCL located in CETJJCL after each metric management execution.

Note: We recommend that you define the CHTSDBMT JCL to an automation product so that it executes automatically when metric management execution ends.

Follow these steps:

1. Edit the CHTSDBMT member of CETJJCL as described in the member.

   CHTSDBMT is ready for execution.

2. Launch your automation product, such as CA OPS/MVS.
3. Define ETJTS601I as a trigger or event message to submit CHTSDBMT. Complete this step using your site-specific practices.

   CHTSDBMT is executed each time message ETJTS601I is received. This JCL submits an online reorganization of the metric data area and defrags the index area of the TSF database.

You have customized the TSF database to optimize database space performance and to reclaim free space after each metric management execution.

Back Up the H2 Database

The CA Chorus H2 database contains several files in the format *file*.h2.db, where *file* is the file name that represents a related set of information, such as policies, metric data, and storage analysis. As a CA Chorus administrator, you are responsible for creating an H2 database backup JCL job and for ensuring that the H2 database backups are taken regularly. Doing so ensures that you retain most of your data if the H2 database fails and an H2 database restore is required.

Prepare the H2 Database Backup

As a CA Chorus administrator, you must perform a one-time setup to prepare for the H2 database backup. This setup includes determining the volume allocation for the H2 database and creating an H2 database backup JCL member. When you are performing this setup, we recommend that you consult with the storage administrator and scheduling administrator.

Follow these steps:

1. Review and gather volume allocation information:
   a. Determine the amount of space that is allocated for the CETJB data set.

      Note: The CETJDB allocation is given in tracks.

   b. Determine where the backup data set will be located.

   c. Verify that the selected location has enough space available for the backup data set, on a single volume or multiple volumes.

      Note: Multiple volume allocations are required when a data set allocation is expected to consume more space than what is available on a single volume. We recommend that you use multiple volumes. Doing so makes it easier to secure the necessary allocation for the H2 database. For more information about multiple volumes, see the *Installation Guide*.

2. Create a JCL member for your H2 database backup and save it to a location that meets your site requirements. The following example provides an outline of what to include in the H2 database backup JCL member:
   a. Delete the previous H2 database backup data set:

      DELETE (*h2_backup_dataset_old*) PURGE

      h2_backup_dataset_old

      Name of the previous H2 database backup data set.

      Example: CHORUS.RUNTIME.H2.PACKAGE

   b. Specify the amount of space that is allocated to the H2 database backup:

      SPACE=(CYL,(*primary_allocation*,*secondary_allocation*),RLSE),

      primary_allocation

      Value of the primary space allocation in cylinders. This value is allocated when the backup data set is created. This file system can grow to be much larger than the original allocation. Therefore, we recommend that you use a primary allocation value that is equal to the current size of the CETJDB data set.

      Example: 1500

      secondary_allocation

Value of the secondary space allocation in cylinders. Use this value if your H2 database backup data set requires more space than what is specified in the primary allocation. This value can be used up to 15 times.

Example: 100

c. Specify your site-specific storage class:

`STORCLAS=`*`storage_class`*`,`

storage_class

Name of your storage class. Typically, this name is the storage class that is used for application backup data sets.

Example: SCWORK

d. Specify the volume allocations that you determined in step 1.

Note: For non-SMS allocations, list the individual volumes in the VOLUME subparameter.

`UNIT=(`*`volume1, volume2`*`)`

volume1

Value for the first volume allocation.

Example: SYSALLDA

volume2

Number of extra units of space for the volume allocation.

Example: 6

e. Specify the data set name for the database file system that you are backing up:

`DATASET(INCLUDE(`*`dataset_for_backup`*`))`

dataset_for_backup

Data set name for the database file system (*INSTALL_HOME*/database) that you are backing up.

Example: CHORUS.RUNTIME.CETJDB

Example

In this example, the bold text indicates the instances where you must specify your configuration values.

```
//* Remove the previous backup
//*
//DELPKG  EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  DELETE (CHORUS.RUNTIME.H2.PACKAGE) PURGE
  SET MAXCC=0
```

```
/*
//*
//PACKAGE EXEC PGM=ADRDSSU
//OUTPUT   DD DSN=CHORUS.RUNTIME.H2.PACKAGE,
//            DISP=(NEW,CATLG,DELETE),
//            SPACE=(CYL,(1500,100),RLSE),
//            STORCLAS=SCWORK,
//            UNIT=(SYSALLDA,6)
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
 DUMP -
      OUTDDNAME(OUTPUT) -
      DATASET(INCLUDE(CHORUS.RUNTIME.CETJDB)) -
      ALLEXCP
/*
//
```

You have determined the volume allocations for the H2 database backup and have created the H2 database backup JCL member.

Run the H2 Database Backup

Important! We recommend that you schedule the H2 database backup job to run regularly, with more frequent backups during system setup.

Follow the backup policy for your site, and consult with your system administrator.

Follow these steps:

1. Verify that the setup for the H2 database backup is complete. See Prepare the H2 Database Backup (see page 66).
2. Verify that you have BPX.SUPERUSR authority. This authority is required to unmount the databases later in this procedure.
3. Delete the *file*.trace.db.old files from the H2 database at *INSTALL_HOME*/database/h2. Repeat this step for each *file*.trace.db.old file in the H2 database. These files contain outdated database activity records that should not be included in the backup.

   `rm INSTALL_HOME/database/h2/file.trace.db.old`

   file

   Name of the file that you are deleting from the H2 database.
4. Stop the JBoss server (CHORJBOS started task):

   `P CHORJBOS`

   A message indicating that the JBoss server started task has ended is logged.
5. If CA Chorus for Storage Management is installed, unmount the CA Chorus for Storage Management database:

   `unmount INSTALL_HOME/database/storage`
6. Unmount the H2 database directory file system:

   `unmount INSTALL_HOME/database`
7. Run the JCL member for the H2 database backup. This JCL member was created in Prepare the H2 Database Backup (see page 66).
8. Mount the H2 database directory file system:

   ```
   mount -t ZFS -o aggrgrow -f
   'chorus_runtime_hlq.CETJDB'  INSTALL_HOME/database
   ```

9. If you unmounted the CA Chorus for Storage Management database, remount it:

   ```
   mount -t ZFS -o aggrgrow -f
   'storage_webclient_derby_db' INSTALL_HOME/database/storage
   ```

   storage_webclient_derby_db

   Name of the CA Chorus for Storage Management Web Client Derby database. To determine the database name, see the E4HI0007 member in CE4HJCL.

   Example: CHORUS.RUNTIME.CE4HVDB

10. Restart the JBoss server (CHORJBOS started task):

    ```
    S CHORJBOS
    ```

    The following message appears when the JBoss server startup is complete:

    ```
    ETJTC001I CA Chorus Startup Complete
    ```

    You have created a backup of the H2 database.

Restore the H2 Database

The CA Chorus H2 database contains several files in the format *file*.h2.db, where *file* is the file name that represents a related set of information, such as policies, metric data, and storage analysis. As a CA Chorus administrator, you can restore the H2 database if the H2 database fails and you have backed up your H2 database. Doing so limits the amount of data that is lost.

Important! We recommend that you perform this procedure only when requested to do so by CA Support.

Create the H2 Database Restore JCL

As a CA Chorus administrator, you must create a JCL member to restore the H2 database. When doing so, we recommend that you consult with the storage administrator and scheduling administrator.

Follow these steps:

Create a JCL member for your restore and save it to a location that meets your site's requirements. The following example provides an outline of what to include in the H2 database restore JCL member:

a. Delete the existing data set for the H2 database directory file system:

   `DELETE (dataset_backup_existing) PURGE`

   dataset_backup_existing

   Data set name for the existing database file system. This name must match the name that you used in your backup job for (DATASET(INCLUDE in the SYSIN DD statement.

   Example: CHORUS.RUNTIME.CETJDB

b. Specify the data set for the H2 database directory file system:

   `INPUT DD DSN=h2_backup_dataset,DISP=SHR`

   h2_backup_dataset

   Data set name for the H2 database directory file system. This name must match the name that you used in your backup job for the OUTPUT DD DSN.

   Example: CHORUS.RUNTIME.H2.PACKAGE

c. (SMS Only) Specify the storage class that is used for the CA Chorus runtime data sets:

   `STORCLAS(storage_class)`

   storage_class

   Storage class name.

   Example: SCPERM

Example

In this example, the bold text indicates the instances where you specify your configuration values.

```
//DELETE   EXEC PGM=IDCAMS
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   *
  DELETE (CHORUS.RUNTIME.CETJDB)      PURGE
  SET MAXCC=0
/*
//DEPLOY EXEC PGM=ADRDSSU
//INPUT    DD DSN=CHORUS.RUNTIME.H2.PACKAGE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
 RESTORE               -
 INDDNAME(INPUT)       -
 DATASET(INCLUDE(**))  -
 REPLACEUNCONDITIONAL  -
 WRITECHECK            -
 STORCLAS(SCPERM)        /*For SMS only*/ -
 CANCELERROR           -
 WAIT(2,2)
/*
//
```

You have created the H2 database restore JCL member.

Run the H2 Database Restore

Important! We recommend that you perform this procedure only when requested to do so by CA Support.

Follow these steps:

1. Verify that you have BPX.SUPERUSR authority. This authority is required to unmount the databases later in this procedure.
2. Stop the JBoss server (CHORJBOS started task):

   ```
   P CHORJBOS
   ```

   A message indicating that the JBoss server started task has ended is logged.
3. If CA Chorus for Storage Management is installed, unmount the CA Chorus for Storage Management database:

   ```
   unmount INSTALL_HOME/database/storage
   ```
4. Unmount the H2 database directory file system:

   ```
   unmount INSTALL_HOME/database
   ```
5. Run the JCL member for the H2 database restore. This JCL member was created in Create the H2 Database Restore JCL (see page 71).
6. Mount the H2 database directory file system:

   ```
   mount -t ZFS -o aggrgrow -f
   'chorus_runtime_hlq.CETJDB'  INSTALL_HOME/database
   ```
7. If you unmounted the CA Chorus for Storage Management database, remount it:

   ```
   mount -t ZFS -o aggrgrow -f
   'storage_webclient_derby_db' INSTALL_HOME/database/storage
   ```

   storage_webclient_derby_db

   Name of the CA Chorus for Storage Management Web Client Derby database. To determine the database name, see the E4HI0007 member in CE4HJCL.

   Example: CHORUS.RUNTIME.CE4HVDB
8. Restart the JBoss server (CHORJBOS started task):

   ```
   S CHORJBOS
   ```

   The following message appears when JBoss server startup is complete:

   ```
   ETJTC001I CA Chorus Startup Complete
   ```

   You have restored the H2 database.

Chapter 4: Discipline-Specific Administration Tasks

How to Add or Remove Storage Engines

CA Chorus connects to each storage engine subsystem through TCP/IP to display object data in the interface. To add or remove storage engine subsystems to CA Chorus, follow these steps:

Note: The storage engine subsystem must be installed and configured before you add it. For more information, see the *CA Chorus for Storage Management Site Preparation Guide*.

1. Stop the CA Chorus task (the JBoss server) by entering the following console command:

   ```
   P CHORJBOS
   ```

   A message indicating that the JBoss server started task has ended is logged.

2. Open the E4HI0010 job for editing. The E4HI0010 job is located in the *chorusstor_runtime_hlq*.CE4HJCL data set.

3. Replicate the *datasource_name* line in the E4HI0010 job for each storage engine subsystem that you want to add, or remove *datasource_name* lines for the storage engine subsystems

   In a multiple storage engine subsystem environment, one storage engine is chosen as the Main (storage) Engine in the CA Chorus Investigator. The Main Engine provides CA Chorus with storage object attributes, which include storage object table header information, the available Administrative Actions for the object, relationships to other objects, and so on.

   CA Chorus determines the Main Engine during JBoss startup. This determination depends on the order of the storage engines that are defined in the E4HI0010 job and if CA Chorus can receive data from the storage engines. That is, the first storage engine that is listed in the E4HI0010 job defaults as the Main Engine during JBoss startup. If a connection to this storage engine is not available during JBoss startup, CA Chorus sets the next storage engine that is listed in the E4HI0010 job as the Main Engine and tries to connect to it. The Main Engine repeats this process until it finds a storage engine to which it can connect and receive data from.

   To use all storage engine features, the Main Engine must have the latest CA Vantage SRM maintenance applied.

Verify the first storage engine listed in the E4HI0010 job contains all user-created Summary Objects, Joined Objects, and so on, and that CA Chorus can connect and receive data from the first storage engine listed in the E4HI0010 job during the JBoss server startup.

Note: For more information about multiple storage engines, see the *CA Chorus for Storage Management User Guide*.

Note: We recommend a maximum of eight storage engine subsystems. If you configure more than eight, you receive a warning message when running the E4HI0010 job. Despite this message, all of your servers will be configured as requested.

4. Substitute the following variables in each replicated *datasource_name* line:

   datasource_name

   Any descriptive name for each storage engine subsystem (maximum 12 characters). Assign each storage engine subsystem with a unique *datasource_name* value. This value is case-sensitive. That is, if you enter it in upper-case, it must be specified as upper case in the Storage Management interface's My Profile Host definition. The value of the *datasource_name* variable is displayed in the HOST column of the Investigator in the object table when the object table is populated with data from multiple hosts.

   Note: Record the *datasource_name* values, exactly as you enter them in this job. You need them later when creating *public* host connection definitions in the Storage Management interface.

   The Storage Management interface accessed from the Quick Links module has only one authenticating host that is used as the single-sign on to this interface. The interface authenticating host name is specified in the *vantage.web.client.host.name* in the CETJOPTN (ENVE4H) member. The value of the *datasource_name* and *vantage.web.client.host.name* can be the same but it is not required.

   ip_address_or_host_name

   The network name or IP Address the storage engine subsystem is running.

   port

   The TCP/IP port number that the storage engine subsystem is listening on for connection requests. This value is set in parameter TCPPORT within each VKGPARMS member of each storage engine subsystem parameter library.

5. Save and submit the E4HI0010 job.

6. Submit either the $TJI0150 or ETJI0150 job in CETJJCL to update the data source XML files with the storage engines.

7. Start the CA Chorus task (the JBoss server):

   ```
   S CHORJBOS
   ```

   A message indicating that the JBoss server is initialized is logged.

The storage engine subsystems are defined for CA Chorus.

How to Change the Cost Analysis Configuration

CA Chorus Cost Analysis comes with a set of standard system analysis scripts that analyze your environment to help you manage your data center costs. The calculations are based on the attribute values in the Customer Site Costs Data object and data provided by the storage engine.

The E4HI0011 job contains industry *norm* defaults, and should have been run during installation. As you use the system and become familiar with the cost analysis scenarios and calculations, configure values that correctly reflect your site so that Costs Analysis can provide you true, meaningful information. You can change the values in the Cost/Value field the following ways:

- Editing the Detail tab Cost/Value field values in the Customer Site Costs Data object using the Investigator
- Editing Cost/Value field values and submitting the E4HI0011 job

Note: For general usage information about Cost Analysis, see the *CA Chorus for Storage Management User Guide*.

To change values in the Cost/Value field using the Investigator

Follow these steps:

1. Open the Customer Site Costs Data object.
2. Select the row containing the value you want to change.
3. Select the value cell of the Cost/Value field that you want to change in the Details pane and select the edit (pencil) icon.
4. Change the value, click Save and then OK.

   The Cost/Value field value is updated in the object and is used in future analysis scenario calculations.

   Note: Changing Cost/Value field values this way does not update the values displayed in the E4HI0011 job.

To change values in the Cost/Value field using the E4HI0011 job

Follow these steps:

1. Copy the E4HJBCRD member to the E4HI0011 job in the *chorusstor_runtime_hlq*.CE4HJCL data set.
2. Follow the instructions in the E4HI0011 job and edit it accordingly to reflect your environment.

   Note: If Cost/Value field values have been changed in the Customer Site Costs Data object using the Investigator, then those values are not displayed in the E4HI0011 job. The Cost/Value field values displayed in the Customer Site Costs Data object are the values used in analysis scenario calculations.
3. Submit the job.
4. Verify that the following return code is received:

   EXPECTED RESULT RC = 0

   The changes are made to Cost Analysis.

   Note: If you change variables and rerun the job after JBoss is started for the first time, you do not have to restart JBoss. That is, you can change variable values and rerun this job at any time and any changes you make are immediately reflected in CA Chorus. Consequently, you do not need to shut down or restart the CA Chorus server before or after rerunning this job.
5. Verify that your changes are activated by reviewing the Cost/Value field values in the Customer Site Costs Data object. This object resides in the Cost Analysis, Base System Analysis directory of the Storage tree in the Investigator.

   A series of analysis scripts are executed once each day. The results from the analysis are visible in the Investigator where you can view the most current executions of these scripts and view up to one year of history (default).

How to Change the Topology Viewer Configuration

CA Chorus for Storage Management lets you view storage object relationships using the Topology Viewer, which provides a graphical view of system resources and their relationships.

A graphical view is useful when you want to see the relationships of storage resources and their dependencies in your storage environment. As you drill down in the Topology Viewer, your storage environment is displayed in a hierarchal, graphic format.

You can change the Topology Viewer default configuration to better display your storage resource environment. For example, the number of DASD volumes that are installed in most environments is large so the Topology Viewer cannot realistically provide a visual representation of each of these volumes on a single mapping. You can change the Topology Viewer configuration to subdivide online DASD volumes. You can also customize online DASD maps where DASD is logically grouped according to various characteristics of the volumes such as by application, line-of-business, and so on.

To change the Topology Viewer configuration, perform the following steps:

1. Copy the member TOPOLVOL from the storage engine CCTUSAMP library to your storage engine parmlib library.
2. Edit the TOPOLVOL member in your parmlib library according to the instructions in the member.
3. Save your changes.
4. Reboot the JBoss server by doing the following:
   a. Stop the JBoss server by entering the following console command:

      ```
      P CHORJBOS
      ```

      A message indicating that the JBoss server started task has ended is logged.

   b. Start the JBoss server:

      ```
      S CHORJBOS
      ```

      A message indicating that startup is complete is logged.

   The Topology Viewer displays storage object relationships according to your configuration.

How to Administer the Storage Management Interface

The system administrator created at least one *public* host for the storage engine subsystem and initialized the Storage Management interface data base during the initial configuration process. If your site has multiple storage engine subsystems, the system administrator can create one *public* host for each additional storage engine subsystem. Individuals can also log in to the public host and add their own private host definitions.

The system administrator can do the following Storage Management interface administration tasks for the Storage Management interface after the configuration phase:

- Manage Public hosts (see page 80)
- Manage Email Server and Number of Concurrent Reports Settings (see page 83)
- Stop and Start the Scheduler (see page 86)
- Manage Scheduled Items (see page 87)

- Manage Public Logo Images (see page 87)
- Manage Public Holiday Schedules (see page 87)
- Create and Manage Public User Views of Source Objects (see page 87)
- Advise users of the web application server schedule time.

  The schedule time is stated in the Scheduler. Users set the schedule time in the Add Timer Schedule dialog that is displayed by the Scheduler Status Window and the Schedule Page of the Customize Report Wizard. This time is dependent on the time that is set for the web application server (the time that is specified in the USS *.profile* file by the system administrator). This time is not necessarily the time on user PCs if users are located in different time zones. Users must consider the time difference when specifying the time in their schedules.

  Inform users that are located in different time zones, the time setting of the web application server. Then they can correctly calculate the schedule time for their reports.

- Advise users of the directory paths for output reports to file, FTP, and web servers.

  When users create output reports or schedule output reports they can specify to output the reports to file, FTP, and web servers. Inform users the directory path from the interface application on the JBoss server to the file, FTP, and web servers to which they want the reports published. If needed, consult your network and security administrator to obtain the information and verify that appropriate write-authority to the server directories is provided.

Manage Storage Management Interface Public Hosts

During configuration, the system administrator created at least one *public* host for the storage engine subsystem and initiated the Storage Management interface. If you add a host to CA Chorus for Storage Management, add the same host to the Storage Management interface as a *public* host.

The system administrator can manage *public* hosts.

Follow these steps:

1. Do one of the following steps:
   - Enter the following URL in your internet browser to start the Storage Management interface outside of CA Chorus:

     `http://<TCPIP address>:<JBOSS Port>/VantageGMI`

     <JBOSS Port> is the HTTPS Connector port. If you used ETJI0105 in CETJJCL to configure the ports, view the job output to determine the port number.

     The line in the job appears similar to the following example:

     `HTTP Connector assigned to port xxxxx`

- Log in to the Storage Management interface from CA Chorus:
  a. Log in to CA Chorus.
  b. Add the Quick Links module to your dashboard.
  c. Click Manage Storage Resources in the Quick Links window.

     The system automatically logs you in to the Storage Management interface and connects you to the storage engine using your mainframe ID.
  d. Click Log Out in the Storage Management interface Menu bar to log off with your mainframe ID.

The Storage Management interface login dialog opens in your browser.

2. 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 on the E4HI0010 job in the *your_chorusstor_hlq*.CE4HJCL data set.

3. Select VantageDB in the Authenticating Hosts field.
4. Click Login.

   The interface opens in your browser with the My Profile window open.

   Note: For an explanation of how to use the My Profile options, click the Help button.

5. Click Add Host Definition to open the New Host Definition dialog.
6. Enter values and make selections in the New Host Definition dialog for the following required fields:

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

   Host Name

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

   Note: The Host Name is case-sensitive. Enter the Host Names exactly as you entered the values for the *datasource_name* variables in the E4HI0010 job in the *your_chorusstor_hlq*.CE4HJCL data set.

   IP Address

   IP address of the back-end storage engine z/OS host. This value is the same as the value of the *ip_address_or_host_name* variable in the E4HI0010 job in the *your_chorusstor_hlq*.CE4HJCL data set.

Port

Port number of the back-end storage engine z/OS host. This value is the same as the value of the *port* variable in the E4HI0010 job in the *your_chorusstor_hlq*.CE4HJCL data set.

Include On Object Tree

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

Use PassTicket

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

- The PassTickets security feature is invoked.
- Automatic login 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, see the *CA Chorus for Storage Management Site Preparation Guide*.

Public Host

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

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

Note: If you plan to activate PassThrough in the *private* host definition, do not define *private* hosts when logged in as the system administrator to the VantageDB authenticating host. You can activate PassThrough in their *private* host definitions. Use the Storage Management interface online help to find out how to use the My Profile options to create *private* hosts after you open the Storage Management interface from the Quick Links module.

7. Click OK.

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

   The public host is added and end users can use it. Repeat steps 4 to 6 to add *public* hosts.

8. Click Logoff.

   The *public* hosts are added to the Storage Management interface and are available for use.

Manage Storage Management Interface Email Server Settings and Concurrent Reports

The system administrator should have set the Storage Management interface email server settings during the configuration process. You can change the email server settings and number of concurrent reports when you log in to the interface as the system administrator.

Email Server Settings

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

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

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

Storage Management interface emails are sent with the sender address of VantageGMIScheduler@ca.com.

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 outgoing connections to port 25 (the SMTP default port). Contact your email administrator, network administrator, or security administrator to discuss the correct values for the Email Server Setting fields.

Number of Concurrent Reports

Storage Management interface generated reports are put in queues when users preview, execute, run, or schedule reports at the same time. The number of queued reports can delay report creation. For scheduled reports, the time of report creation can be later than the scheduled time.

Reports can be generated as follows:

- Reports can be *scheduled* to run using the interface Scheduler Status Window and the Customize Report Wizard.
- Reports can be *previewed* (immediately) using the interface Preview option on the Customize Report Wizard.
- Reports can be *generated* (immediately) using the interface Run option on the Scheduler Status Window or the Execute option on the Customize Report Wizard.
- Reports are sent with sender address VantageGMIScheduler@ca.com.

Reports generated by the Preview, Run, and Execute options are referred to as *ad-hoc* reports.

The performance of the report executor program depends on the number of concurrent report threads that are defined in this Number of Concurrent Reports field. The default and minimum number of report threads is 2. Where one thread is reserved for execution of ad-hoc reports and one thread is for scheduled reports.

Follow these steps:

1. Do one of the following steps:
   - Enter the following URL in your internet browser to start the Storage Management interface outside of CA Chorus:

     `http://<TCPIP address>:<JBOSS Port>/VantageGMI`

     <JBOSS Port> is the HTTPS Connector port. If you used ETJI0105 in CETJJCL to configure the ports, view the job output to determine the port number.

     The line in the job appears similar to the following example:

     `HTTP Connector assigned to port xxxxx`
   - Log in to the Storage Management interface from CA Chorus:
     a. Log in to CA Chorus.
     b. Add the Quick Links module to your dashboard.
     c. Click Manage Storage Resources in the Quick Links window.

        The system automatically logs you in to the Storage Management interface and connects you to the storage engine using your mainframe ID.
     d. Click Log Out in the Storage Management interface Menu bar to log off with your mainframe ID.

   The Storage Management interface login dialog opens in your browser.
2. 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 on the E4HI0010 job in the *your_chorusstor_hlq*.CE4HJCL data set.
3. Select VantageDB in the Authenticating Hosts field.
4. Click Login.

   The interface opens in your browser with the My Profile window open.
5. Close the My Profile window.
6. Click Tools and then Application Configuration to open the Application Configuration dialog.

   Note: Only the system administrator can use the Application Configuration dialog.

7. Enter email server information and set the number of concurrent reports in the following fields:

   Email Server

   (Required) The DNS name or IP address of your email server which is used by the interface to relay email messages. The interface sends email directly to the recipient's email server using the SMTP protocol.

   Port

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

   The interface sends emails for the following:

   - With output report attachments.
   - Report generation failure messages.

   Default: 25. However, some sites use a different value, for example, 587.

   User Name

   (Optional) Enter the user ID that has authority to send email from the designated email server. This field is for sites that have 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 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.

   Number of Concurrent Reports

   The performance of the report executer program depends on the number of concurrent report threads that are defined here.

   Valid Range: 2 through 5

   Default: 2, where one thread is reserved for execution of ad-hoc reports and one thread is for scheduled reports.

   Important! The system report creator can be CPU- and memory-intensive. Increasing the maximum number of reports that can be run concurrently can improve report execution performance. However, reports can operate upon a vast amount of data, and memory and system resources can be impacted. Verify that your system resources (for example, memory), are configured appropriately to handle the increased concurrent load. If this value is set to a value greater than 2, you should monitor memory and system resources.

8. Click OK to save your settings and close the Application Configuration dialog.

9. Click Log Out.

   The Storage Management interface email server settings and number of concurrent reports are specified.

How to Stop and Start the Storage Management Interface Scheduler

The Storage Management interface Scheduler manages scheduled tasks defined by users. For example, users can schedule reports for periodic output to servers and as attachments to emails. You might need to stop the Scheduler, manage user-scheduled items using the Schedule Status Window, and restart the Scheduler. For example, when users mistakenly scheduled many large reports too frequently which cause a system overload.

When the Scheduler is stopped no scheduled items are performed. When the Scheduler is restarted, scheduling resumes.

The system administrator can stop and restart the Scheduler:

1. Do one of the following steps:
   - Enter the following URL in your internet browser to start the Storage Management interface outside of CA Chorus:

     `http://<TCPIP address>:<JBOSS Port>/VantageGMI`

     <JBOSS Port> is the HTTPS Connector port. If you used ETJI0105 in CETJJCL to configure the ports, view the job output to determine the port number.

     The line in the job appears similar to the following example:

     `HTTP Connector assigned to port xxxxx`
   - Log in to the Storage Management interface from CA Chorus:
     a. Log in to CA Chorus.
     b. Add the Quick Links module to your dashboard.
     c. Click Manage Storage Resources in the Quick Links window.

        The system automatically logs you in to the Storage Management interface and connects you to the storage engine using your mainframe ID.
     d. Click Log Out in the Storage Management interface Menu bar to log off with your mainframe ID.

   The Storage Management interface login dialog opens in your browser.

2. 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 on the E4HI0010 job in the *your_chorusstor_hlq*.CE4HJCL data set.

3. Select VantageDB in the Authenticating Hosts field.
4. Click Login.

   The interface opens in your browser with the My Profile window open.

5. Close the My Profile window.
6. Click Tools in the interface Menu bar, and then Stop Scheduler or Start Scheduler.

   Note: At Storage Management interface application server startup, the scheduler is automatically started. If you are logged in as the system administrator, the Start Scheduler option shows as disabled if the scheduler is already started.

   The Scheduler is stopped or restarted.

7. Click Log Out.

   You are logged out of the interface.

Additional Storage Management Interface Administrator Tasks

The system administrator can perform additional administrator tasks when logged in to the interface VantageDB authenticating host.

Perform the following steps to log in to the interface VantageDB authenticating host as the system administrator.

Follow these steps:

1. Do one of the following steps:

   - Enter the following URL in your internet browser to start the Storage Management interface outside of CA Chorus:

     `http://<TCPIP address>:<JBOSS Port>/VantageGMI`

     <JBOSS Port> is the HTTPS Connector port. If you used ETJI0105 in CETJJCL to configure the ports, view the job output to determine the port number.

     The line in the job appears similar to the following example:

     `HTTP Connector assigned to port xxxxx`

- Log in to the Storage Management interface from CA Chorus:
  a. Log in to CA Chorus.
  b. Add the Quick Links module to your dashboard.
  c. Click Manage Storage Resources in the Quick Links window.

     The system automatically logs you in to the Storage Management interface and connects you to the storage engine using your mainframe ID.
  d. Click Log Out in the Storage Management interface Menu bar to log off with your mainframe ID.

The Storage Management interface login dialog opens in your browser.

2. 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 on the E4HI0010 job in the *your_chorusstor_hlq*.CE4HJCL data set.

3. Select VantageDB in the Authenticating Hosts field.
4. Click Login.

   The interface opens in your browser with the My Profile window open.

5. Use the appropriate Tool menu item to manage the following:

   Manage Scheduled Items

   Manage all scheduled items, such as reports scheduled to run periodically, using the Schedule Status Window. Users can only manage their scheduled items, they cannot manage scheduled items created by other users. The Scheduler Status Window lists all activities scheduled to run including activity details. For more information about the Schedule Status Window, click the Help button.

   Manage *Public* Logo Images

   Manage *Public* Logo Images using the Logo Image Manager. The Logo Image Manager lists all Private (images owned by end users) and Public logo images. Observe the following:

   - End users can apply *public* logos to their output reports using the Customize Report Wizard.
   - The report creator does not resize the logo image. The report creator publishes the logo image on reports in the size you upload it. Therefore, upload the logo image in the appropriate size.

- Logo images in the following formats are supported:
  - PNG
  - BMP
  - GIF
  - JPG

Note: For more information about the Logo Image Manager, click the Help button.

Manage *Public* Holiday Schedules

Manage *Public* Holiday Schedules using the Holiday Manager. *Public* Holiday Schedules are the dates that scheduled output reports skip and the output reports are not produced.

Note: For more information about the Holiday Manager, click the Help button.

Create and Manage *Public* User Views of Source Objects

All users can display all *Public* user views. Only the system administrator can save user views of source objects as Public user views of source objects. To create and manage *Public* user views you must connect to a storage engine host after you are logged in as the system administrator:

a. Connect to a storage engine host by clicking the host in the object tree and entering your normal host user ID and password.

b. Open the source object you want to base the *Public* user view on.

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

d. Make your settings in the wizard dialogs.

Note: For more information about the wizard dialogs, click the Help button.

e. In the Save Options wizard dialog, select the Save as... option.

The Save Options wizard dialog expands.

f. Enter a name and description of the *public* user view and select Save As Public User View.

The *public* user view is created in the VantageDB, and is available for all users.

6. Log out of the Storage Management interface.

Additional system administrator tasks are completed.

Chapter 5: Managing CA Chorus Logs

How to Change the Log Threshold for All Executions

As a system administrator, you can edit the log level or threshold without restarting the JBoss server. Doing so changes the log level for all executions.

Note: All log files are located in /cai/cetjr3m0/logs by default.

Add the following JBoss property to the ENVETJ member of *chorus_runtime_hlq*.CETJOPTN (before the lines to *Export all Java SDK options*):

jboss.server.log.threshold

Specifies the log level or threshold on a running JBoss server. The log level determines the amount of information that is written to the log files. These log messages appear in the following log files: server.log, server-ebcdic.log, chorus-status.log, and chorus-query.log.

Values: ERROR, WARNING, INFO, DEBUG, and TRACE (in ascending order by amount of detail).

Default: INFO (DEBUG and TRACE categories are not logged).

Important! DEBUG and TRACE log levels can cause high CPU usage and increased disk space usage. Use these values only under the direction of CA support. We recommend that you do not use this property to implement DEBUG or TRACE. In emergency situations, you can enter a command to set the level to DEBUG. See the example in How to Change the Log Level (see page 92).

Save your changes.

The ENVETJ member is updated and the changes are applied as applicable to the CA Chorus log file.

Example: Change Log Threshold

In this example, the log level is set to DEBUG:

```
IJO="$IJO -Djboss.server.log.threshold=DEBUG"
```

How to Change the Log Level Temporarily

As a CA Chorus administrator, you can temporarily change the log level on a running JBoss server through a z/OS console command. The log level determines the amount of information that is written to the log files.

To change the log level from the z/OS console, specify the following command and press Enter:

Important! DEBUG and TRACE log levels can cause high CPU usage and increased disk space usage. Use these values only under the direction of CA support. We recommend that you only use this command to change the level to DEBUG during an emergency. For all standard scenarios, the recommended method is to use this command to temporarily change the log level, and revert it back to the default (INFO) once done with the investigations. In rare cases when you must use DEBUG for all the executions, the recommended best practice is to update the ENVETJ threshold (see page 91).

```
F CHORJBOS,APPL=LOGLEVEL=level
```

CHORJBOS

Specifies the job name of the CA Chorus server.

Default: CHORJBOS

level

Specifies the level of detail for information that is written to the log files.

Values: FATAL, ERROR, WARN, INFO, DEBUG, and TRACE (in ascending order by amount of detail).

Default: INFO (DEBUG and TRACE categories are not logged).

Messages are generated that describe the command that was entered and the change that was made to the log level.

Example: Set the Log Level to DEBUG

This example shows the command to enter on the z/OS console to set the log level for the server to DEBUG:

```
F CHORJBOS,APPL=LOGLEVEL=DEBUG
```

The following messages are displayed on the console log:

```
ETJTC008I Modify command entered: LOGLEVEL=DEBUG
ETJTC009I Changing log level to DEBUG
```

How to Log Metrics Panel Data

As a CA Chorus administrator, you can log metric data each time a new data point is added to the Metrics panel. Doing so helps you debug issues with the metric data. The logged metric data includes the details of all charts in the Metrics panel and the data points for each of these charts. This metric data is logged in the server.log file.

Important! Metric data is logged in the server.log file each time that data is added to the Metrics panel. If your site frequently adds data to the Metrics panel, the server.log file can grow quickly. Use this setting only under the direction of CA Support.

Note: All log files are located in /cai/cetjr3m0/logs by default.

Follow these steps:

1. Edit the following system property in the ENVETJ member of *chorus_runtime_hlq*.CETJOPTN:

   ```
   IJO="$IJO -Dcom.ca.chorus.logMetricsData=enable_log"
   ```

   enable_log

   Specifies whether Metrics panel data is generated and logged in the server.log file.

   Values: True (enable logging) or False (disable logging)

   Default: False

   Example:

   In this example, we enable logging the Metrics panel data:

   ```
   IJO="$IJO -Dcom.ca.chorus.logMetricsData=true"
   ```

2. Save your changes.
3. Start the JBoss Server (CHORJBOS started task) to activate the system property:

   ```
   S CHORJBOS
   ```

   The following message appears when the JBoss Server startup is complete:

   ```
   ETJTC001I CA Chorus Startup Complete
   ```

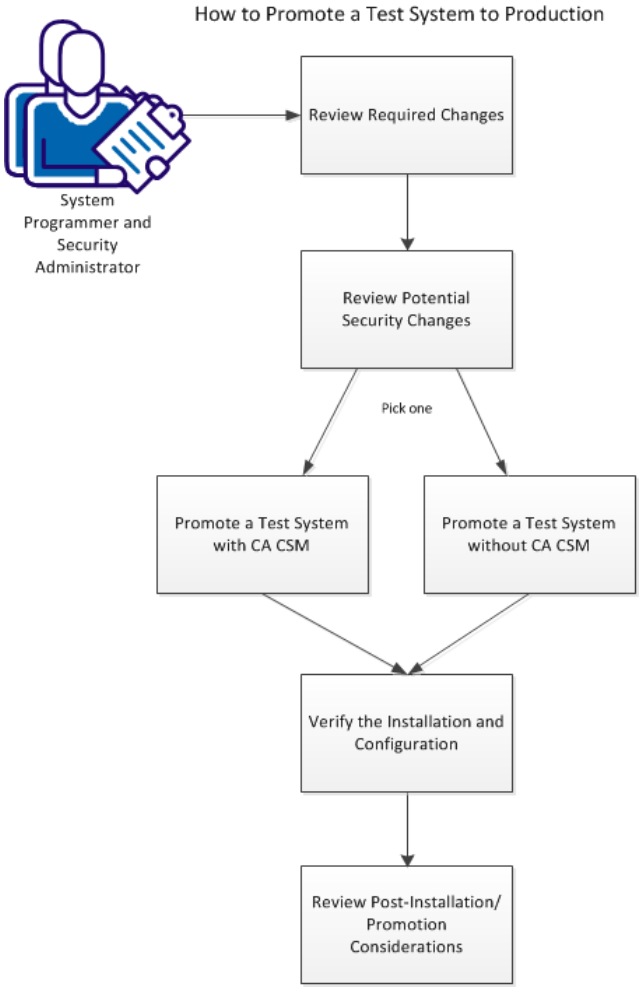
The ENVETJ member is updated, and the changes are applied as applicable to the server.log file.

Chapter 6: How to Promote a Test System

Many sites install CA Chorus into a test system for initial vetting. As a system programmer, you want to promote CA Chorus to production for widespread use at your company.

This scenario shows how a system programmer and security administrator promote CA Chorus to a production environment with or without CA Chorus™ Software Manager. For this scenario, the procedures leave your test system intact. You will have a second system (production) under a new high-level qualifier.

Important! Do not begin this scenario until all team members have a clear understanding of their responsibilities.



Complete these tasks:

1. Review Required Changes.
2. Review Potential Security Changes. (see page 99)
3. Choose one of the following options:
   - Promote a Test System with CA CSM. (see page 105)
   - Promote a Test System without CA CSM. (see page 110)
4. Verify the Installation and Configuration (see page 118).
5. Review Post-Installation/Promotion Considerations (see page 120).

Review Required Changes

General

The following items must be changed if the test and product system are on the *same LPAR*:

- High-level qualifier (HLQ) for the deployed libraries
- UNIX System Services (USS) Runtime Home
- CHORTSF or CHORTSFR instances running on the same LPAR
  - By design, CHORTSF and CHORTSFR communicate across two LPARs and require the same SUFFIX. However, within a single LPAR, multiple CHORTSF or CHORTSFR instances cannot share a SUFFIX.
  - By default, the suffix is PROD. For a second TSF instance on the same LPAR, you need a new suffix. The commands to make this change appear later in this scenario.

Maintenance

Confirm that CA Chorus, its disciplines, and back-end systems have all current maintenance applied.

Port range

CA Chorus has the following port requirements for the JBoss server and Time Series Facility (TSF) components:

- 12 consecutive ports for the CA DSI Server and JBoss server. The JBoss ports consist of one DSI two-way (connecting and listening) port, and 11 server (listening) ports.
- Three one-way ports for TSF (These ports do not need to be consecutive with each other or with the 12 ports from the previous bullet).

  Note: If TSF instances are being used on a remote LPAR, two more one-way ports are required for the instance.

  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.

These ports are configured later in the installation during the JBoss server and TSF configuration.

To confirm that the ports you intend to use are available, consult your network management team.

Database

You must create a CA Datacom/AD/CA Chorus MUF. The CA Datacom/AD library may be shared, but you must create a separate CA Datacom/AD CUSLIB for the new CA Chorus environment. For the steps to create a MUF, see the CA Datacom/AD documentation.

H2 Database

Do not copy the H2 database (profile database) into a new environment. When you configure the new environment, JBoss creates an H2 database.

User Documentation

Evaluate any user documentation that has been indexed. Following the promotion, you can index this content in the new environment.

Important! Do not share the user doc file systems between two CA Chorus systems because you cannot mount a file system at two locations.

Started task names

Identify which of the follow uses cases matches your site:

- If the systems are running on a *different LPAR*, you can use the same Started Task Names. If you do so, place the procs for the started tasks in a separate proclib from the original location.
- If the systems are on the *same LPAR*, the started task names must be different. The procs can be in the same proclib.

Back-end system

You may want to access a different back-end system for some disciplines. For the instructions to establish access to the back-end systems, see the applicable *Site Preparation Guide*.

Review Potential Security Changes

Before you continue, identify your site use case:

- Option A: You are using the same External Security Manager (ESM) database for the existing configuration *and* the new environment.
- Option B: You are using a new ESM for your new environment.

Reuse ESM

Resource definitions

This list assumes that you are using the same ESM database for the existing configuration *and* the new environment.

- User IDs: CHORADM / CHORTHD
- APPLIDs: Use the same APPLIDs for CA Chorus and discipline resources.
- PassTickets: Existing passtickets are sufficient provided the user IDs and APPLIDs are not changed.

CHORADM Access

If the new HLQ is not included in the existing rules that give CHORADM access to data sets, give CHORADM access to the same files (low-level name) under the new HLQ. For more information, see the ETJI095*x* security job. *x* equals A for CA ACF2, T for CA Top Secret, or R for IBM RACF. The file resides in CETJJCL of the currently installed system.

Note: After you review this topic, go to the applicable deployment procedure in this scenario.

New ESM

1. Locate the applicable ETJI095*x* security job. *x* equals A for CA ACF2, T for CA Top Secret, or R for IBM RACF. The file resides in CETJJCL of the currently installed system.

   Note: The job files reside on the CA Chorus product page under Content Type, Recommend Reading.

2. Run the security job (see page 100).
3. Verify that the new environment has the same BPX facilities as the original configured environment.

   Note: You may need to assign CA Chorus resources to users IDs who plan to access it in the new environment. For the steps to authorize users, see the *Site Preparation Guide*. You can add the authorizations after the new environment is up and running.

4. Confirm that the security requirements for the back-end systems are met. If you reuse the same back-end systems, no changes are necessary.
5. Start the applicable deployment procedure.

Run the CA Chorus Platform Security Job

The ETJI095*x* security job simplifies how you meet many security requirements. The security job is identified as follows: ETJI095*x*, where x equals A for CA ACF2, T for CA Top Secret, or R for IBM RACF. These jobs reside on the CA Chorus product page under Content Type, Recommended Reading.

This job and section apply only to CA Chorus platform security. The discipline *Site Preparation Guides* address additional security.

The following list details the security requirements that the job addresses.

Important! Review the following conceptual material before you proceed to the steps at the *end of this topic*.

(CA Top Secret only) Master Facility

If you are using CA Top Secret, define a master facility and associate it with the CA Chorus started task. Use CAWEBSVR as the master facility. The master facility (MASTFAC keyword) lets users access the CAWEBSVR facility. Before you can use the facility as a master facility, define it to CA Top Secret as a user facility in the system facilities matrix.

Important! Perform this task only once. If you have added CAWEBSVR to the facilities matrix and you have activated the definition, do not repeat this task.

You then give permission to the CA Top Secret facility CAWEBSVR for every user ACID accessing CA Chorus.

Administrator User ID and Group ID

You run CA Chorus using one user ID (CHORADM by default), which has a defined UNIX System Services (USS) segment, so that the following conditions are met:

- The user ID has a valid UID that is *not* UID(0).
- The shell is specified as the default shell, typically /bin/sh.
- The user ID has a valid OMVS group.

Note: We recommend that the home directory be the same as the CA Chorus installation path.

The following security user IDs are created when you run the ETJI095*x* job. If the default values are not used, change all occurrences of CHORADM and CHORGRP in the security job.

CHORADM

Started task user ID that is used to run CA Chorus.

CHORGRP

Default group name. This group creates a relationship among all relevant security objects.

CHORTHD

User ID for PassTicket requests related to applications.

Note: Unique USS UIDs and GIDs (user ID and group ID numbers) must be used for the CA Chorus started task user IDs. Select a UID and GID that numerically match to track them easier.

Important! All users, including the installer, must have access to the group specified in this member. The default group is CHORGRP.

Started Tasks

The following started tasks are defined when you run the ETJI095*x* job. The default values are shown. If you do not use default names for the started tasks, change the names in the security job.

Note: We recommend that all CA Chorus tasks run as a started task with REGION=0M. If your site restricts the REGION=0M parameter, we recommend that you run with the maximum region size permitted.

your_muf_name

Started task name that is associated with the CA Datacom/AD MUF for CA Chorus. The name depends on the name that you previously assigned to the MUF.

CHORTSF

Started task name that is associated with the Time Series Facility (TSF).

CHORTSFR

Started task name that is associated with the remote TSF configuration. This started task is created only if TSF data relays are defined.

CHORJBOS

Started task name that is associated with the JBoss server.

Resource Class

CA Chorus defines security resources in class CAMFC, which you define using your security product. You then assign permissions for users to the discipline-specific resources as applicable. For more information about the required user permissions, see the discipline-specific installation guides.

Note: CAMFC is a resource class specifically for CA Chorus. The name of the class and entries cannot be modified.

PassTickets for General Users

PassTickets are required for users to access the z/OS components and products that CA Chorus and its supported disciplines use. A *PassTicket* is a temporary encoded and encrypted substitute for the user password that can be used to access a specific application. The PassTicket must be used within 10 minutes of the time it is generated.

Using PassTickets enables the z/OS components and products to authenticate a user ID without sending z/OS passwords through the network. Instead, the user is authenticated after they first log in with a valid z/OS user ID and password. The following process occurs when the user selects a function that accesses a z/OS component:

- The CA Chorus web service calls the z/OS security product to generate a PassTicket for access authorization.
- The PassTicket is sent with the user request to the component, possibly on a different z/OS system.

  The component calls the z/OS security product to authenticate the user using the PassTicket as a password substitute before processing the request.

The CA Chorus server generates PassTickets that permit users to access the various back-end products that the CA Chorus disciplines use. As users access components, PassTickets are generated to validate the requests.

The CA Chorus PassTicket configuration includes the following systems:

- One z/OS system running the JBoss server and the back-end products (like CA Detector, CA Compliance Manager, CA Vantage SRM, and CA NetMaster NM for TCP/IP) that are required for the CA Chorus disciplines on the same system. This type of system is a CA Chorus server system.
- Additional z/OS systems running only the products and components that the CA Chorus disciplines require. This type of system is known as a CA Chorus remote system.

The CA Chorus server system provides the entry point for CA Chorus users. Users can then access all of the CA Chorus remote systems that they have been authorized to use in your network of z/OS systems.

The PassTicket configuration for the security product must be done on each z/OS system that is hosting a component that CA Chorus uses. Configure PassTickets in your z/OS security products to enable the generation and validation of connections that are required for CA Chorus disciplines. If your site meets the following criteria, no additional security setup is required on the remote systems:

- The security products in your z/OS configuration are using a shared security database.
- You want to add one or more remote systems, only the CA Chorus server system setup is required.

If the requisite products and components exist on a remote system that does not share the security database, additional security setup is required on the remote systems.

PassTickets for CA CSM Users

CA Chorus uses PassTicket security to let users launch CA Chorus™ Software Manager from the Quick Links module without requiring another user login. All systems using Passtickets must have identical application names and session keys for all nodes on the network. Note the following requirements:

- If your CA Chorus instance and CA CSM instance reside on *different* machines, after you run this job, complete the applicable steps in How to Configure CA CSM Passtickets for CA Chorus.
- If your CA Chorus instance and CA CSM instance reside on the *same* machines, after you run this job, CA CSM passticket configuration is complete, with one exception. If you are using CA ACF2, complete the one CA Chorus server side and CA CSM side step in Sample: Use CA ACF2 to Configure PassTickets for Connecting to CA Chorus™ Software Manager from CA Chorus.

Follow these steps:

1. Retrieve the ETJI095*x* job that applies to your external security manager. These jobs reside on the CA Chorus product page under Content Type, Recommended Reading.
2. Review member ETJI095*x* in its entirety.
3. Edit the job according to the member comments.
4. Submit the member.

   The noted security requirements are met.
5. (CA Top Secret only) Add the following lines to the applicable CA Top Secret parameter file (PARMFILE):

   ```
   FACILITY(USERxx=NAME=CAWEBSVR)
   FACILITY(CAWEBSVR=PGM=********)
   FACILITY(CAWEBSVR=ACTIVE,SHRPRF,MULTIUSER,AUTHINIT)
   ```

   xx

   User facility number. Use any available user facility number on your system.

   Important! The xx value must match the value that you specified when you ran ETJI095T.

Promote a Test System with CA CSM

For this method, you plan to deploy and configure the new environment using CA CSM.

As you complete the new deployment and configuration, wizards guide you through process. As you move through the wizard, update components per the required changes (see page 97).

Important! When you deploy, you **must** use a new high-level qualifier (HLQ) for the new environment. Failure to do so could erase your existing deployment.

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.

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 118) and Post Installation Considerations.

   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.

Note: To finalize this scenario, go to Verify the Installation and Configuration (see page 118).

Promote a Test System without CA CSM

For this method, you plan to deploy and configure the new environment using manual deployment and automated-configuration (auto config).

Important! When you deploy, you **must** use a new high-level qualifier (HLQ) for the new environment. Failure to do so could erase your existing deployment.

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.

Configure Your Product for Promotion (Auto Config)

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

Follow these steps:

Note: Complete these steps from your new deployment directory.

1. Locate your existing test environment configuration data set (Configuration_ds file).
2. Submit ETJICUST in *your_chorus_hlq*.CETJJCL with the high-level qualifier (HLQ) that you specified during the manual deployment.

   The expected return code is zero. You now have a new configuration data set (environment) that is the basis for your production environment.
3. Copy the contents of your existing (original) configuration data set into the new configuration data set.
4. Modify this data set for the required changes (see page 97).
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. You submit the preconfigured jobs from this location.

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.

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)

      Note: As part of the CA Datacom/AD prerequisite, the following libraries should 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

l. If you have a CHORTSF instance, which resides on same the LPAR as the original, it must use a different SUFFIX.

   a. Add the TSFSUFFIX=*c*|*n* parameter to the TSFPARMS member in CETJOPTN, using a one-character alphabetic (c) or numeric (n) identifier for the TSF region. The valid values are A to Z, or 0 through 9.

   b. Add the export TSFII='c|n' parameter to the ENVETJ member in *chorus_2.5_runtime_hlq*.CETJOPTN. This statement specifies a one-character alphabetic (c) or numeric (n) identifier for the TSF region in the JBoss environment settings. This value must match the value that is specified for TSFSUFFIX. The value must be in single quotes.

m. Start TSF (/S CHORTSF).

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

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

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, submit ETJI0135 from *custom_hlq*.CETJJCL.

r. (Optional) If you want to add a CA Chorus™ Software Manager link to the Quick Links module, submit ETJI0140 from *custom_hlq*.CETJJCL. 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.

s. (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 outside of CA CSM.

   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 125).

   e. Enable DB2 object migration. Complete the steps in How to Enable DB2 Object Migration (see page 130).

      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)

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 following two steps, run the 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.

   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. Complete the tasks in Verify the Installation and Configuration (see page 118) and Post Installation Considerations.

   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/Promotion 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 identified content that you want to index in the new environment, complete the indexing scenario in the *Product Guide*.
- You may need to assign CA Chorus resources to users IDs who plan to access it in the new environment. For the steps to authorize users, see the *Site Preparation Guide*.
- If you added a TSF SUFFIX, update the discipline suffix.

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

1. Configure the Cost Analysis (see page 135): 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 135): 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 to finalize the configuration. Doing so lets the Policy Administration interface send alerts to the Alerts module.

Add the TSF Suffix to the Disciplines

To update the disciplines to add the TSF suffix to feed data to more than one TSF instance, complete the following tasks:

- For CA Chorus for DB2 Database Management, update the TPDTFEED started task to send data to the additional instance.

  Note: For more information about updating TPDTFEED, see the *CA Chorus Manual Configuration Guide*.

- For CA Chorus Infrastructure Management for Networks and Systems, update the suffix as noted in this discipline's *Site Preparation Guide*.

- For CA Chorus for Security and Compliance Management, update the TSFSUFF parameter in CA ACF2 or the CHORUSTSFSX parameter in CA Top Secret to send data to the additional instance.

  Note: For more information about these parameters, see the *CA ACF2 Administration Guide* or *CA Top Secret Control Options Guide*.

- For CA Chorus for Storage Management, update the CHTSFSUF parameter in CA Vantage SRM to send data to the additional instance.

  Note: For more information about CHTSFSUF, see the *CA Vantage SRM Configuration Guide*.

Appendix A: 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.

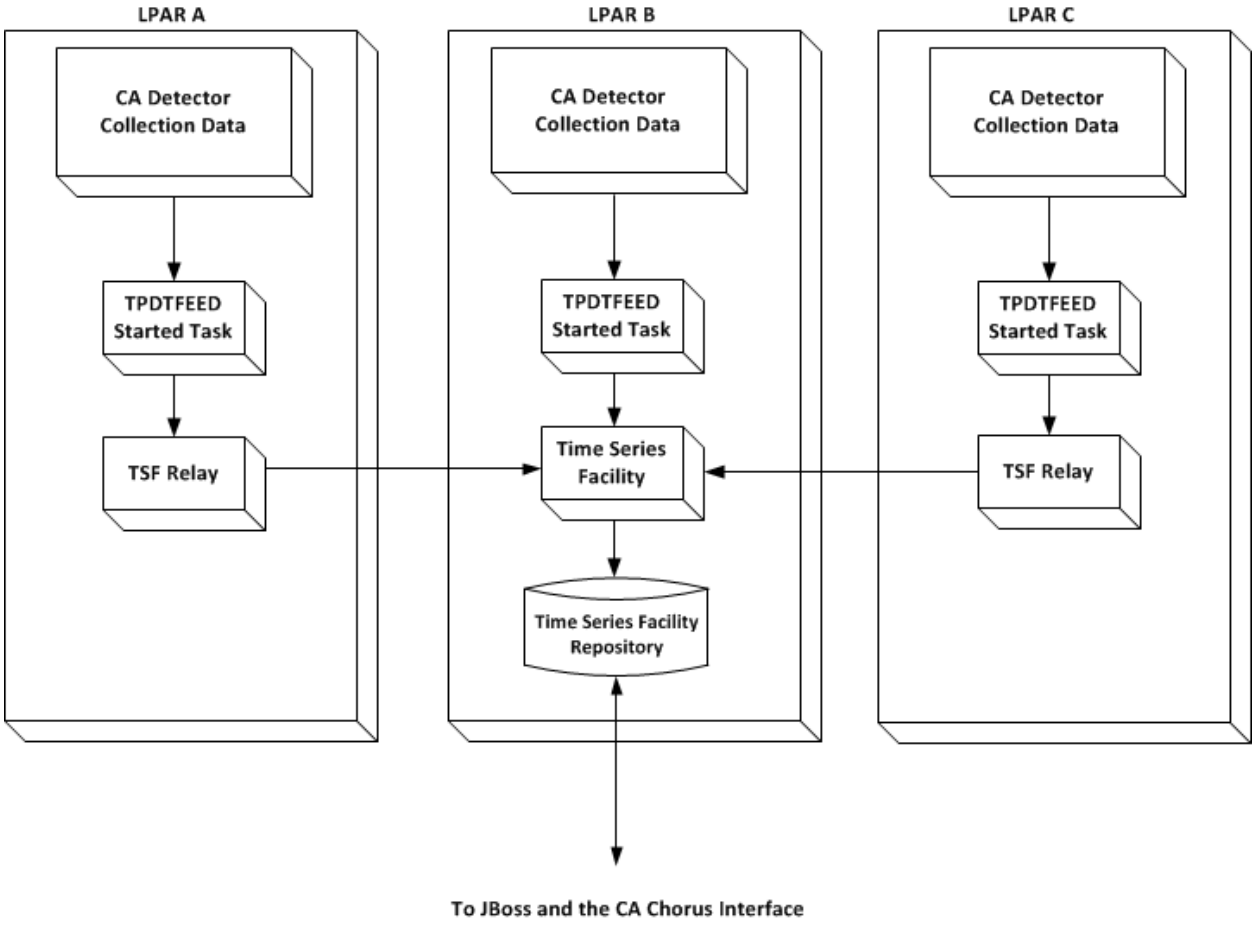
CA Detector Statistics Gathering Overview

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, create [set the rcm variable for your book] models and the Object Migrator configuration PDS and members. In addition, update the OFAPROC started task, and MJETJOM model JCL.

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 OFAPROC started task ID needs READ permission for BPX.SERVER.

Note: 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. The OFAPROC started task was created and customizing during the configuration of the Object Framework Services agent (OFA) during the installation of the CA Database Management Solutions for DB2 for z/OS. For more information about configuring the OFA agent, see the *CA Database Management Solutions for DB2 for z/OS Installation Guide*.

Note: To execute the [set the rbp variable for your book], 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. Create a default model for global configuration and optional user-specific models for individual user configurations by completing the following steps using [set the rcm variable for your book]:

   Note: Any @DEFAULT model can be used.

   a. Type **PROF** on the [set the rcm variable for your book] Main Menu and press Enter.

      The Expert Profile panel appears.

   b. Type **6** for Utility Model Services on the Option line and press Enter.

      The General Model Services panel appears.

   c. Type **T** next to an existing model to create a template (copy).

      The General Model Utilities panel appears.

d. Specify a name for the model in the Model ID field and press PF3.

   The model is created and saved with the name (model ID) and creator. These models are used during the DB2 object migration when the migration is submitted for analysis.

2. Create the Object Migrator configuration data set (*config.om.pds*) and members by completing the following steps:

   a. Create the Object Migrator configuration PDS with the following attributes:

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

      The configuration PDS is defined.

   b. Create an @DEFAULT member in the configuration PDS and optional members for each Object Migrator user.

      The members appear in the configuration data set members list. Object Migrator user members override global settings that are defined in the @DEFAULT member.

   c. Add the following JCL to the @DEFAULT member, replacing the italicized text with site-specific values:

      Note: The members must include the desired JOB statement for z/OS batch jobs and the model name and creator.

      ```
      <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>
      ```

      Note: Use the JOB statement, model name (ID), and creator values for overriding global settings that are defined in the @DEFAULT member. For more information about overriding high-level qualifiers for work data set allocations, see the *CA Chorus for DB2 Database Management User Guide*.

<JOB CARD> </JOB CARD>

Specifies the JOB statement details.

<MODEL4></MODEL4> and <MODEL4C>/</MODEL4C>

Specifies information that is required for the Object Migrator configuration including the model ID and creator. The model ID specifies an existing [set the rcm variable for your book] model name. Specify @DEFAULT for the global configuration member. If you created models, the model ID and creator must match the models that you created. The creator specifies the model creator user ID.

Save your changes.

The @DEFAULT global configuration member is created.

d. Repeat the previous step.

The JCL is added to the individual user members.

3. Update the OFAPROC started task JCL:

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.

4. 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 B: 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 C: Additional CA Chorus for Security and Compliance Management Configuration

Configure the Global Configuration

Configure the global configuration to specify CA Compliance Manager 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.
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, log location, and log level under Alerts.

   Note: Using SSL for alerts is optional. Your environment must be configured before you can use this option. For more information about enabling SSL, see the *CA Chorus for Security and Compliance Management Site Preparation Guide*.

   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 CA Compliance Manager 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 CA Compliance Manager 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 CA Chorus Application Server. 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

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.

Use SSL

(Optional) Lets you use SSL for alerts. Your environment must be configured before you can use this option. For more information about setting CA Compliance Manager components, see the *CA Chorus for Security and Compliance Management Site Preparation Guide*.

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 CA Compliance Manager.

Default Route Code

Specifies the default routing code that is used for the WTO messages sent by the CA Compliance Manager.