CA Chorus™

Administration Guide

Version 04.0.00, Fourth Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA ACF2™ for z/OS (CA ACF2)
- CA Chorus™
- CA Chorus™ for IMS 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 NetMaster® Network Management for TCP/IP (CA NetMaster NM for TCP/IP)
- CA OPS/MVS® Event Management and Automation (CA OPS/MVS)
- 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 third edition of this documentation:

- Global—Updated to clarify the TSF behavior.
- How to Promote a Test System (see page 55)—Noted that CAMFC resource class and entries cannot be modified.

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

- New Time Series Facility and TSF Bridge (see page 25)—Updated this topic to clarify the TSF behavior.
- Global—Removed Optional from the TSF Bridge (CHORTSFB) step.
- Removed the Modify the Session Timeout topic as this feature is no longer supported.

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

- How to Log Metrics Panel Data (see page 53)—Added this topic to describe how to log Metrics panel data in the server.log file.
- How to Promote a Test System (see page 55)—Added links to the ETJI095x security jobs on CA Support Online.

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

- Start the CA Chorus Components (see page 9) and Stop the CA Chorus Components (see page 11)—Added the commands for the TSF Server (CHORNTSF) and TSF Bridge (CHORTSFB).
- Modify the Started Task JCL for the ARM Wrapper (see page 22)—Updated the procedure to include the start commands for the TSF Server (CHORNTSF) and TSF Bridge (CHORTSFB).
- New Time Series Facility and the TSF Bridge (see page 25)—Added this topic to explain this new configuration.
- Time Series Facility Heap Memory Recommendations (see page 27)—Added this topic to provide TSF heap memory size recommendations.
- Time Series Facility Database Recommendations (see page 29)—Updated this topic to provide TSF database size recommendations for the Version 4.0 TSF.
- How to Customize the Time Series Facility Database (see page 30)—Updated this scenario as follows:

- Added a description of the TSF purge process.
- Added a procedure to expand the zFS that contains the TSF database using the JCL member TSFZGROW.
- Added a procedure to calculate the TSF data store size.

- Back Up the TSF Database (see page 35) and Restore the TSF Database (see page 38)—Added procedures for backing up and restoring the TSF database.
- Back Up the H2 Database (see page 41) and Restore the H2 Database (see page 46)—Updated procedures for TSF requirements.
- How to Promote a Test System
  - Updated for TSF changes.
  - Added a step to restart CA Top Secret.
- Global—Renamed the JBoss server to the CA Chorus Application Server.

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 CA Chorus Application Server and the Time Series Facility (TSF). 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 TSF Bridge:

   ```
   S CHORTSFB
   ```

   A message indicating that the TSF Bridge is initialized is logged.

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

2. Start the TSF Server:

   ```
   S CHORNTSF
   ```

   A message indicating that the TSF Server is initialized is logged.

   ```
   ETJTS001I *** TSF SERVER STARTUP COMPLETE ***
   ```

3. (Optional) Start the TSF Relay:

   Important! This command is required if you are using a relay for remote LPARs **and** you are using a TSF Bridge.

   ```
   S CHORTSFR
   ```

   A message indicating that the TSF Relay is initialized is logged.

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

4. Start the CA Chorus Application Server:

   ```
   S CHORJBOS
   ```

   A message indicating that startup is complete is logged.

   ```
   ETJTC001I CA Chorus Startup Complete
   ```

More information

Time Series Facility and TSF Bridge (see page 25)

How to Stop CA Chorus

You can stop the CA Chorus components independent of the back-end products supporting each discipline. 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:

- CA Chorus Application Server
- Time Series Facility (TSF)
- TSF Relay

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 CA Chorus Application Server by entering the following console command:

   ```
   P CHORJBOS
   ```

   A message indicating that the CA Chorus Application server started task has ended is logged.

2. Stop the TSF Bridge:

   ```
   P CHORTSFB
   ```

   A message indicating that TSF Bridge has ended is logged.

3. Stop the TSF Server:

   ```
   P CHORNTSF
   ```

   A message indicating that TSF Server has ended is logged.

4. (Optional) Stop the TSF Relay:

   Important! This command is required if you are using a relay for remote LPARs and you are using the TSF Bridge.

   ```
   P CHORTSFR
   ```

   A message indicating that the TSF Relay has ended is logged.

More information

Time Series Facility and TSF Bridge (see page 25)

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 CA Chorus Application Server. The CA Chorus administrator must perform this procedure.

Follow these steps:

1. Stop the CA Chorus Application Server:

   ```
   P CHORJBOS
   ```

   A message indicating that the CA Chorus Application Server started task has ended is logged.

2. 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 CA Chorus Application server session timeout configuration
   IJO="$IJO -Dchorus.jboss.session.timeout.minutes=45"
   ```

3. Start the CA Chorus Application Server:

   ```
   S CHORJBOS
   ```

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

Note: You will not be able to modify session timeout value if you have enabled auto refresh or if you have configured metrics and alerts.

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 CA Chorus Application Server:

   ```
   P CHORJBOS
   ```

   A message indicating that the CA Chorus Application Server started task has ended is logged.

3. Start the CA Chorus Application Server:

   ```
   S CHORJBOS
   ```

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

Chapter 2: Managing High Availability

How to Implement HA Automatic Restart Management

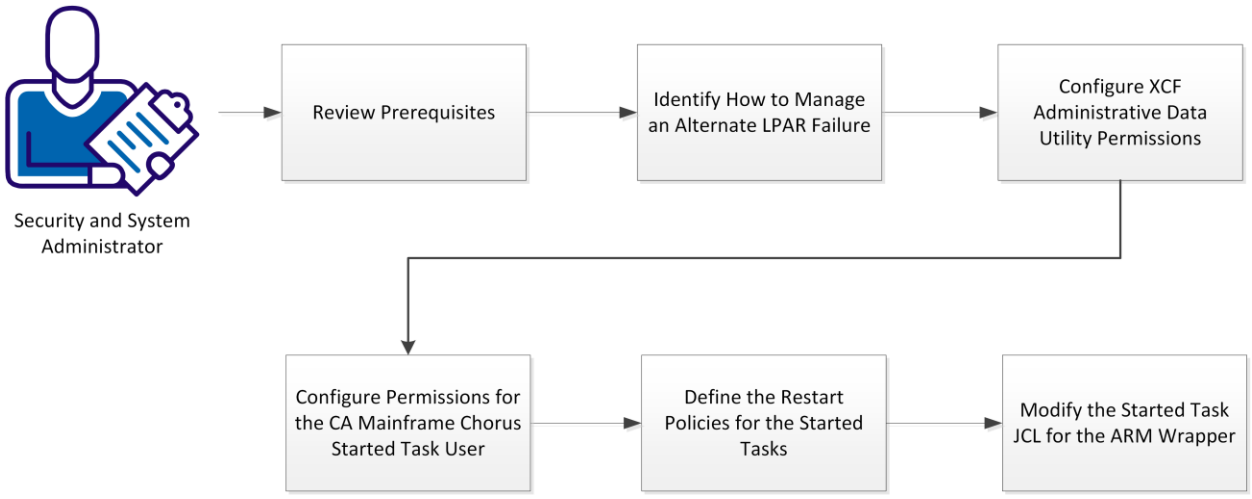
High Availability (HA) is a system design approach such that when a system fails, users can continue working on another system. For example, if the LPAR fails where CA Chorus is running, users need instant access to a secondary LPAR running the product.

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 16)
2. Identify How to Manage an Alternate LPAR Failure. (see page 17)
3. Configure XCF Administrative Data Utility Permissions (see page 18).
4. Configure Permissions for the CA Chorus Started Task User. (see page 20)
5. Define the Restart Policies for the Started Tasks (see page 22).
6. Modify the Started Task JCL for the ARM Wrapper (see page 22).

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 Application server, mount the product zFS file systems on the alternate LPAR before the CA Chorus Application Server 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 CA Chorus Application Server step.

Because the CA Chorus Application Server only starts on the alternate LPAR when the primary LPAR fails, do not mount the file systems in another location when the alternate CA Chorus Application 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 CA Chorus Application 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.

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.

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*.

Important! In the following content, CHORTSFB indicates the TSF Bridge started task; CHORNTSF indicates the TSF Server started task.

Follow these steps:

1. Edit the ARM parameters in the following members in *chorus_runtime_hlq*.CETJJCL as described in the member and save your changes:
   - CHORJBOS member
   - Each of the TSF members for the corresponding TSF tasks that you plan to use:
     - CHORNTSF member
     - CHORTSFB member
     - CHORTSFR member

   The started task JCL is updated.
2. Copy the CHORJBOS, CHORTSFB, and CHORNTSF 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 Bridge (CHORTSFB) is copied to an LPAR where a TSF Relay (CHORTSFR) runs, stop the TSF Relay to let the TSF Bridge 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. (Optional) If you have TSF relays on other LPARs, update their CETJOPTN(TSFRPRMS) member to point to the new TTSFHOST.
5. Start the TSF Bridge:

   ```
   S CHORTSFB
   ```

   A message indicating that the TSF Bridge is initialized is logged.

   ```
   N00503 *** TSF INITIALIZATION COMPLETE TSF ***
   ```
6. Start the TSF Server:

   ```
   S CHORNTSF
   ```

   A message indicating that the TSF Server is initialized is logged.

   ```
   ETJTS001I *** TSF SERVER STARTUP COMPLETE ***
   ```
7. (Optional) Start the TSF Relay:

   Important! This command is required if you are using a relay for remote LPARs **and** you are using a TSF Bridge.

   ```
   S CHORTSFR
   ```

   A message indicating that the TSF Relay is initialized is logged.

   ```
   N00503 *** TSF INITIALIZATION COMPLETE TSF ***
   ```
8. Restart the CHORJBOS started task:

   ```
   S CHORJBOS
   ```

The following message appears when the CA Chorus Application Server 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

Time Series Facility and TSF Bridge

The Time Series Facility (TSF) stores the data that the mainframe products collect and provide. The TSF provides a single point for the collection, storage, management, and organization of the product data. You can use the TSF for analyzing your product data, and reporting. TSF data is collected on a periodic basis, which provides useful information about parameters such as performance or usage. Version 4.0 introduces a simplified TSF architecture while maintaining the robust User Interface (UI).

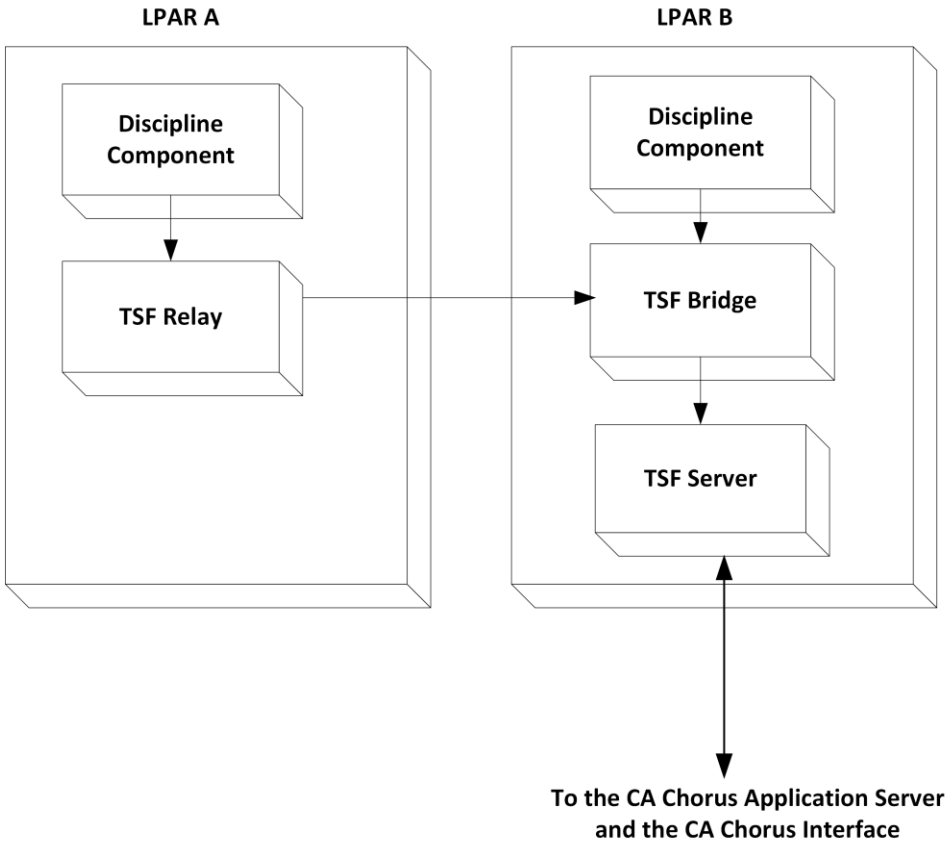
In all releases before Version 4.0, CA Datacom/AD housed the TSF database. The back-end products and CA Chorus then communicated with this database using a TSF Server. Version 4.0 introduces a TSF architecture that eliminates the CA Datacom/AD database, thus simplifying data management and configuration tasks. In this new architecture, the database resides on a file system under the CA Chorus installation. You must route your TSF connections from the CA Chorus disciplines to a TSF Bridge. This bridge then sends your data to the TSF Server. Ultimately, all TSF data reaches the new TSF Server and is housed in its database (not in a CA Datacom/AD database). Therefore, the TSF documentation includes commands and procedures that are related to the TSF Bridge (CHORTSFB) and the new TSF Server (CHORNTSF).

Exceptions

Application developers can push data to the TSF Server using APIs (C or Assembler). If you are a Software Development Kit user, you decide the API to use. This new TSF architecture uses only the CHORNTSF started task. To use the new TSF architecture, configure your application to talk directly to the TSF Server (hostname and port), bypassing the TSF Bridge.

The following diagram shows these TSF configurations:

- LPAR A: Uses the TSF Bridge and TSF Relay on a remote LPAR.
- LPAR B: Uses the TSF Bridge on a local LPAR.



Time Series Facility Heap Memory Recommendations

We recommend that you allocate 250-300 MB of heap memory for the Time Series Facility (TSF) Server with the following additional TSF heap recommendations for each discipline:

- 250 MB for CA Chorus for Security and Compliance Management.
- 450-800 MB for CA Chorus for Storage Management based on an average *entity instance* count of 5,000-17,500.

  entity instance

  Unique name of a dfSMS and non-dfSMS storage volume name, DASD volume name, catalog name, or data set group name that is registered in CA Vantage.
- 360-600 MB for CA Chorus Infrastructure Management for Networks and Systems based on an average of 12-36 LPARs.

Note: The recommended values are based on average usage. You can calculate the amount of TSF heap memory that is required based on your system load. For the equations to calculate your TSF heap memory, see the *Troubleshooting Guide*.

To modify the TSF heap memory size, see the Java heap size (Java SDK Option) setting in the ENVNTSF member of *chorus_runtime_hlq*.CETJOPTN. For the heap range, -Xms is the starting value (lower end of the range), and -Xmx is the ending value (higher end of the range).

Example: Minimum Recommendations

- TSF Server with all disciplines: 250 MB + 250 MB + 450 MB + 360 MB = 1,310 MB
- TSF Server with the Security and Storage disciplines: 250 MB + 250 MB + 450 MB = 950 MB

Example: Optimum Recommendations

- TSF Server with all disciplines: 300 MB + 250 MB + 800 MB + 600 MB = 1,950 MB
- TSF Server with the Security and Storage disciplines: 300 MB + 250 MB + 800 MB = 1,350 MB

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 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.
- CA SYSVIEW and CA NetMaster NM for TCP/IP supply data for CA Chorus Infrastructure Management for Networks and Systems.

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.

Time Series Facility Database Recommendations

We recommend that you allocate a minimum of 3,000 cylinders for the Time Series Facility (TSF) database with the following additional recommendations for each discipline:

Note: These recommendations assume a retention period of 30 days and a cylinder size of 720 KB. If you lengthen the retention period or decrease the cylinder size, we recommend that you increase the database size.

CA Chorus for Security and Compliance Management

- 700 cylinders

CA Chorus for Storage Management

- Lower bound (assumes 5,000 *entity instances*): 930 cylinders
- Upper bound (assumes 17,500 *entity instances*): 3,150 cylinders

entity instances

Unique name of a dfSMS and non-dfSMS storage volume name, DASD volume name, catalog name, or data set group name that is registered in CA Vantage.

CA Chorus Infrastructure Management for Networks and Systems

- Lower bound (assumes 12 LPARs): 17,471 cylinders
- Upper bound (assumes 36 LPARs): 52,413 cylinders

Given that each site and configuration can vary significantly, use these recommendations as a general reference as you plan your TSF database sizing activities.

Best Practice for TSF Database Sizing

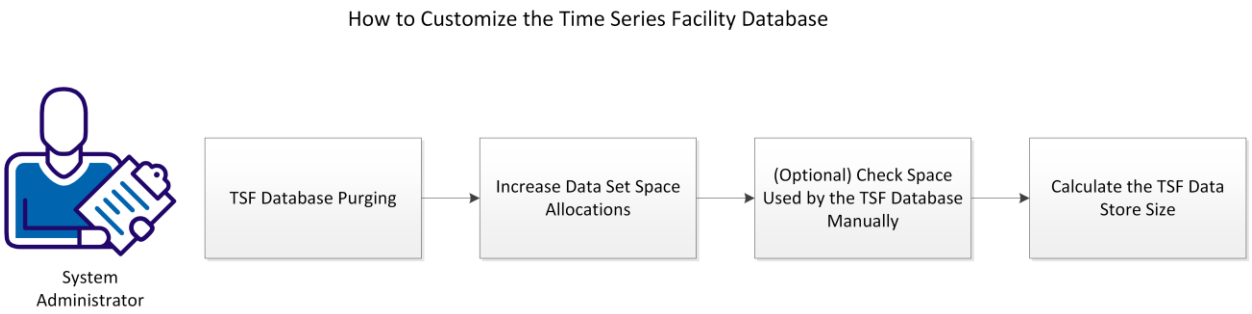
Use the initial allocation of 3,000 cylinders as a test space for determining the actual amount of TSF database space that your site requires. To do so, monitor the TSF database space for a few days to determine the appropriate TSF database size for your site. To increase your TSF database space, see Increase Data Set Space Allocations (see page 31).

Note: You can also calculate the TSF database size using the algorithm that is provided in Calculate TSF Data Store Size (see page 33).

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:



Perform the following tasks to customize the TSF database:

1. Review the process of TSF Database Purging (see page 30).
2. Increase Data Set Space Allocations (see page 31).
3. (Optional) Check Space Used by the TSF Database Manually (see page 32).
4. Calculate the TSF Data Store Size (see page 33).

TSF Database Purging

The TSF database uses large amounts of disk space. To avoid the TSF database from becoming full, CA Chorus monitors the TSF database space. When the zFS containing the TSF database reaches approximately 90 percent capacity, CA Chorus automatically purges the oldest 10 percent of the TSF data.

The automatic purge of TSF data from the zFS is not user configurable. When the TSF data purge begins, CA Chorus issues informational message ETJTS006I. When the TSF data purge is complete, CA Chorus issues informational message ETJTS007I.

Note: For more information about the TSF purge messages, see the *Message Reference Guide*.

Increase Data Set Space Allocations

System administrators can add space to the TSF database if CA Chorus is purging TSF data more often than you would like. Adding more space enables continuous use of the database when the data area is full.

Note: For more information about the TSF database purging process, see TSF Database Purging (see page 30).

Follow these steps:

1. Edit the following environment variables in the TSFZGROW job in *chorus_runtime_hlq*.CETJJCL. These environment variables are located under STDENV in the ZGROW step.

   a. Set the following environment variable to expand the zFS that contains the TSF database:

      GROW_SIZE_KB

      Specifies the number of kilobytes (KB) to expand the zFS by. The zFS expands to the nearest rounded-up number of cylinders. For example, with a cylinder size of 720 KB, any GROW_SIZE_KB between 1-719 KB expands the zFS by 720 KB, or one cylinder.

      Limits: A non-zero number.

   b. Set the following environment variable to verify the NTSF data set:

      NTSF_DATASET

      Specifies the pointer to the NTSF data set that was defined during the CA Chorus installation and that is currently mounted.

2. Submit the member TSFZGROW.

   Note: To run this job, you must have the required permissions to access and modify the zFS. These permissions are defined in the *Site Preparation Guide*.

You have successfully increased space in the zFS that contains the TSF database and helped to ensure continuous operation of the database.

(Optional) Check Space Used by the TSF Database Manually

CA Chorus monitors the TSF database space and automatically purges the oldest 10 percent of the TSF data when the TSF database reaches 95 percent capacity.

You can manually check the space that the TSF database uses. To do so, enter the following command from the UNIX System Services (USS) directory:

```
df -P <INSTALL_HOME>/database/ntsf
```

If CA Chorus is purging TSF data more often than you would like, add space to the TSF database. For more information about adding space to the TSF database, see Increase Data Set Space Allocations (see page 31).

Calculate the TSF Data Store Size

To help you determine how much space to allocate to the Time Series Facility (TSF) data store, use this algorithm. The TSF data store refers to the allocation parameters for the zFS that houses the TSF database.

Note: For the TSF database size recommendations, see Time Series Facility Database Recommendations (see page 29).

Follow these steps:

Note: This algorithm assumes a 3390 KB cylinder size.

1. Calculate the TSF data store space that is required for an entity:

   ```
   Unique_metric_count = entityInstanceCount * metricCountInEntity
   Metric_Count_Gathered = (TIME_STORAGE_IN_DAYS*24*60*60 / METRIC_SEND_RATE)
   SPACE_REQUIRED_B = SPACE_REQUIRED_B + (Unique_metric_count * 4) *
   Metric_Count_Gathered
   ```

   entityInstanceCount

   Indicates the total number of expected instances of the entity that is reporting to the TSF Server.

   Note: An entity is an object that is defined by one or more primary key columns. A unique combination of the entity's primary key columns forms an entity instance. For example, an *entity* that is named CPU has primary keys LPAR and SYSPLEX. This entity has two *entity instances* that are named CPU_a and CPU_b. CPU_a has primary keys LPAR="LPAR11" and SYSPLEX="PLEX11." CPU_b has primary keys LPAR="LPAR31" and SYSPLEX="PLEX31."

   metricCountInEntity

   Indicates the total number of metrics in the entity.

   TIME_STORAGE_IN_DAYS

   Indicates the number of days to retain data in the TSF database. This value should be the same for all entities.

   Example: 7 days

   METRIC_SEND_RATE

   Indicates the entity-specific rate (in seconds) at which metrics are sent.

   Example: 60 seconds

   SPACE_REQUIRED_B

   Indicates the running total of the space (in bytes) that is required for each entity that you are sending to the TSF Server. For the first entity, the value is 0. For each additional entity, the value is the sum of all entity instances that you have calculated so far.

2. Repeat step 1 for each entity that you are gathering metrics for.

3. Calculate the total recommended size for the TSF data store:

   SPACE_REQUIRED_CYL = RoundUp (*SPACE_REQUIRED_B* / *BYTES_PER_CYLINDER*) + 124

   SPACE_REQUIRED_B

   Indicates the running total of the space (in bytes) that is required for each entity that you are sending to the TSF Server. For the first entity, the value is 0. For each additional entity, the value is the sum of all entity instances that you have calculated so far.

   BYTES_PER_CYLINDER

   Indicates the number of bytes per cylinder on the target DASD.

You have calculated the total space (in cylinders) that is required for the TSF database.

Example:

In this example, we assume the following information:

- The BYTES_PER_CYLINDER is 849,960.
- You want to retain the TSF data for 7 days.
- Sysview Entity 1:
  - Your Sysview role has an entity sending 200 metrics every 60 seconds.
  - This entity has 41 unique entity instances.
- Sysview Entity 2:
  - Your Sysview role has an entity sending 20 metrics every 60 seconds.
  - The entity has 20 unique entity instances.

1. Calculate the TSF data store space that is required for Sysview Entity 1:

   ```
   Unique_metric_count = 200*41 -> 8200
   Metric_Count_Gathered = (7*24*60*60 / 60) -> (7*24*60) -> 10080
   SPACE_REQIURED_B = 0  [no previous SPACE_REQUIRED_B value] + (8200*4) * 10080 ->
   330,624,000 Bytes (~315MB)
   ```

2. Calculate the TSF data store space that is required for Sysview Entity 2:

   ```
   Unique_metric_count = 20*20 -> 400
   Metric_Count_Gathered = (7*24*60*60 / 60) -> (7*24*60) -> 10080
   SPACE_REQUIRED_B = 330,624,000 [value from entity 1 calculation] + (400*4) * 10080
   -> 346,752,000 Bytes (~330MB)
   ```

3. Calculate the total size of the TSF data store:

   ```
   SPACE_REQUIRED_CYL = 346,752,000 [total for both entities] / 849,960 + 124 ->
   531.96 -> 532 Cylinders
   ```

   The value of the SPACE_REQUIRED_CYL is the total space (in cylinders) that is required for the TSF data store. In this example, the TSF database requires 532 cylinders.

You have customized the TSF database to optimize database space performance.

Back Up the TSF Database

The CA Chorus TSF database contains mapdb and H2 files. As a CA Chorus administrator, you are responsible for creating a TSF database backup JCL job and for ensuring that the TSF database backups are taken regularly. Doing so ensures that you retain most of your data if the TSF database fails and a TSF database restore is required.

Prepare for the TSF Database Backup

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

Follow these steps:

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

       Note: The CETJNTSF 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 TSF database. For more information about multiple volumes, see the *Installation Guide*.

2. Create a JCL member for your TSF 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 TSF database backup JCL member:

   a. Delete the previous TSF database backup data set:

      DELETE (*tsf_backup_dataset_old*) PURGE

      tsf_backup_dataset_old

      Name of the previous TSF database backup data set.

      Example: CHORUS.RUNTIME.TSF.PACKAGE

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

      SPACE=(CYL,(*primary_allocation*,*0*),RLSE),

      primary_allocation

      Value of the primary space allocation in cylinders. This value is allocated when the backup data set is created. The administrator sets the value of the original TSF database that was created during CA Chorus configuration based on metrics requirements. However, the administrator may have increased the size of the file system to prevent metric purging. Therefore, we recommend that you use a primary allocation value that is equal to the current size of the CETJNTSF data set.

      Example: 1500

   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/ntsf) that you are backing up.

Example: CHORUS.RUNTIME.CETJNTSF

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.TSF.PACKAGE) PURGE
  SET MAXCC=0
/*
//*
//PACKAGE EXEC PGM=ADRDSSU
//OUTPUT   DD DSN=CHORUS.RUNTIME.TSF.PACKAGE,
//            DISP=(NEW,CATLG,DELETE),
//            SPACE=(CYL,(1500,0),RLSE),
//            STORCLAS=SCWORK,
//            UNIT=(SYSALLDA,6)
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
 DUMP -
      OUTDDNAME(OUTPUT) -
      DATASET(INCLUDE(CHORUS.RUNTIME.CETJNTSF)) -
      ALLEXCP
/*
//
```

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

Run the TSF Database Backup

Important! We recommend that you schedule the TSF 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 TSF database backup is complete. See Prepare the TSF Database Backup (see page 35).
2. Verify that you have BPX.SUPERUSR authority. This authority is required to unmount the databases later in this procedure.
3. Stop the TSF Server (CHORNTSF started task):

   ```
   P CHORNTSF
   ```

4. Unmount the TSF Server database:

   ```
   unmount INSTALL_HOME/database/ntsf
   ```

5. Run the JCL member for the TSF database backup. This JCL member was created in Prepare the TSF Database Backup (see page 35).
6. Remount the TSF Server database:

   ```
   mount –t ZFS –f 'chorus_runtime_hlq.CETJNTSF'
   INSTALL_HOME/database/ntsf
   ```

7. Restart the TSF Server (CHORNTSF started task):

   ```
   S CHORNTSF
   ```

   You have created a backup of the TSF database.

Restore the TSF Database

The CA Chorus TSF database contains mapdb and H2 files. As a CA Chorus administrator, you can restore the TSF database if the TSF database fails and you have backed up your TSF 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 TSF Database Restore JCL

As a CA Chorus administrator, you must create a JCL member to restore the TSF 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 TSF database restore JCL member:

a. Delete the existing data set for the TSF 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.CETJNTSF

b. Specify the backed-up data set for the TSF database directory file system:

   `INPUT DD DSN=tsf_backup_dataset,DISP=SHR`

   tsf_backup_dataset

   Backed-up data set name for the TSF 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.TSF.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.CETJNTSF)      PURGE
  SET MAXCC=0
/*
//DEPLOY EXEC PGM=ADRDSSU
//INPUT    DD DSN=CHORUS.RUNTIME.TSF.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 TSF database restore JCL member.

Run the TSF 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 TSF Server (CHORNTSF started task):

   ```
   P CHORNTSF
   ```

3. Unmount the TSF Server database:

   ```
   unmount INSTALL_HOME/database/ntsf
   ```

4. Run the JCL member for the TSF database restore. This JCL member was created in Create the TSF Database Restore JCL (see page 39).

5. Remount the TSF Server database:

   ```
   mount -t ZFS -f 'chorus_runtime_hlq.CETJNTSF'
   INSTALL_HOME/database/ntsf
   ```

6. Restart the TSF Server (CHORNTSF started task):

   ```
   S CHORNTSF
   ```

   You have restored the TSF database.

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 42).
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 CA Chorus Application Server (CHORJBOS started task):

   `P CHORJBOS`

   A message indicating that the CA Chorus Application Server started task has ended is logged.
5. Stop the TSF Server (CHORNTSF started task):

   `P CHORNTSF`
6. If CA Chorus for Storage Management is installed, unmount the CA Chorus for Storage Management database:

   `unmount INSTALL_HOME/database/storage`
7. Unmount the TSF Server database:

   `unmount INSTALL_HOME/database/ntsf`
8. Unmount the H2 database directory file system:

   `unmount INSTALL_HOME/database`
9. Run the JCL member for the H2 database backup. This JCL member was created in Prepare the H2 Database Backup (see page 42).
10. Remount the H2 database directory file system:

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

11. 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

12. Remount the TSF Server database:

    ```
    mount -t ZFS -f' chorus_runtime_hlq.CETJNTSF'
    INSTALL_HOME/database/ntsf
    ```

13. Restart the TSF Server (CHORNTSF started task):

    ```
    S CHORNTSF
    ```

14. Restart the CA Chorus Application Server (CHORJBOS started task):

    ```
    S CHORJBOS
    ```

    The following message appears when the CA Chorus Application 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 CA Chorus Application Server (CHORJBOS started task):

   ```
   P CHORJBOS
   ```

   A message indicating that the CA Chorus Application Server started task has ended is logged.
3. Stop the TSF Server (CHORNTSF started task):

   ```
   P CHORNTSF
   ```
4. If CA Chorus for Storage Management is installed, unmount the CA Chorus for Storage Management database:

   ```
   unmount INSTALL_HOME/database/storage
   ```
5. Unmount the TSF Server database:

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

   ```
   unmount INSTALL_HOME/database
   ```
7. Run the JCL member for the H2 database restore. This JCL member was created in Create the H2 Database Restore JCL (see page 47).

8. Remount 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. Remount the TSF Server database:

    ```
    mount -t ZFS -f' chorus_runtime_hlq.CETJNTSF'
    INSTALL_HOME/database/ntsf
    ```

11. Restart the TSF Server (CHORNTSF started task):

    ```
    S CHORNTSF
    ```

12. Restart the CA Chorus Application Server (CHORJBOS started task):

    ```
    S CHORJBOS
    ```

    The following message appears when CA Chorus Application Server startup is complete:

    ```
    ETJTC001I CA Chorus Startup Complete
    ```

    You have restored the H2 database.

Chapter 4: Managing CA Chorus Logs

How to Change the Log Level for All Executions

As a system administrator, you can edit the log level or threshold without restarting the CA Chorus Application Server. Doing so changes the log level for all executions.

Note: All log files are located in /cai/cetjr4m0/logs by default.

Add the following 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 CA Chorus Application 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.

Save your changes.

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

Example: Change Log Level

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 CA Chorus Application 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 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.

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

CHORJBOS

Specifies the job name of the CA Chorus Application 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/cetjr4m0/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 CA Chorus Application Server (CHORJBOS started task) to activate the system property:

   ```
   S CHORJBOS
   ```

   The following message appears when the CA Chorus Application server startup is complete:

   ```
   ETJTC001I CA Chorus Startup Complete
   ```

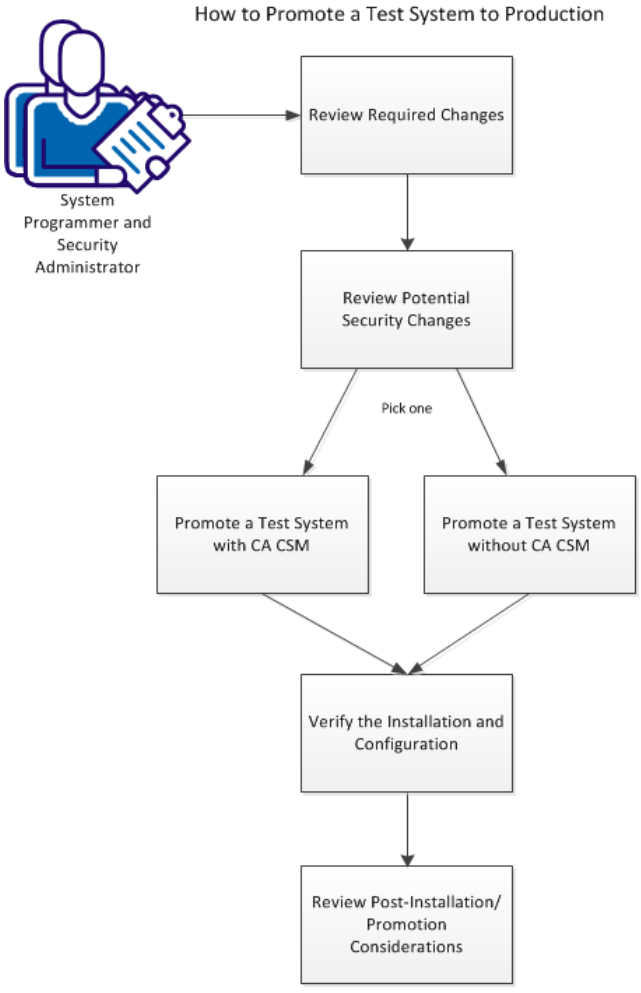
The ENVETJ member is updated, and the changes are applied as applicable to the server.log file.

Chapter 5: 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. (see page 57)
2. Review Potential Security Changes. (see page 59)
3. Choose one of the following options:
   - Promote a Test System with CA CSM. (see page 66)
   - Promote a Test System without CA CSM. (see page 71)
4. Verify the Installation and Configuration. (see page 78)
5. Review Post-Installation/Promotion Considerations (see page 80).

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
- CHORNTSF, CHORTSFB, or CHORTSFR instances running on the same LPAR
  - By design, CHORNTSF, CHORTSFB, and CHORTSFR communicate across two LPARs and require the same SUFFIX. However, within a single LPAR, multiple CHORNTSF, CHORTSFB, 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 CA Chorus Application Server and Time Series Facility (TSF) components:

- Thirteen consecutive ports for the CA DSI server and CA Chorus Application server. The CA Chorus Application Server ports consist of one DSI two-way (connecting and listening) port, and 12 server (listening) ports.
- Two ports for the TSF Server. These ports are server (listening) ports similar to the 12 CA Chorus Application Server ports that are noted in the previous bullet.
- One one-way port for the TSF Bridge. (This port does not need to be consecutive with the 13 ports for the CA DSI server and CA Chorus Application Server.) You can specify an actual value (port number), or you can omit the value to let the TSF Bridge dynamically assign a port number.

  Note: If the TSF Bridge instances are being used on a remote LPAR, one more one-way port is required to receive data from a relay. You must specify an actual value; dynamic assignment is not supported.
- One one-way port for the TSF Relay. (This port does not need to be consecutive with the 13 ports for the CA DSI server and CA Chorus Application Server.) You can specify an actual value (port number), or you can omit the value to let the TSF Bridge dynamically assign a port number.

Note: The TSF Remote Relay uses an additional 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.

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

H2 Database

Do not copy the H2 database (profile database) into a new environment. When you configure the new environment, the CA Chorus Application server 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 ETJI095x 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 ETJI095x 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 security job files also reside on the CA Chorus product page under Content Type, Recommended Reading: ETJI095A for CA ACF2, ETJI095T for CA Top Secret, or ETJI095R for IBM RACF.

   Note: On CA Support Online, the links to the Version 4.0 security jobs are appended with two letters instead of one to differentiate these jobs from the Version 3.0 security jobs: ETJI095AC for CA ACF2, ETJI095TS for CA Top Secret, and ETJI095RA for IBM RACF.

2. Run the security job (see page 60).
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,* ETJ2540T, and ETJ3040*x* security jobs simplify how you meet many security requirements. You run *one* of these jobs depending on your installation type and external security manager.

Note: In these security jobs, 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.

- ETJI095*x* for new installations, or for upgrades where you use a unique CA Chorus Administrator ID (CHORADM) for the Version 4.0 region.
- ETJ2540T for upgrades where you use the same CHORADM for the Release 2.5 and Version 4.0 regions and are using CA Top Secret.
- ETJ3040*x* for upgrades where you use the same CHORADM for the Version 3.0 and Version 4.0 regions.

Important! These jobs and this section apply only to CA Chorus Platform security. The discipline *Site Preparation Guides* address additional security requirements. Before proceeding with this topic, determine if your discipline offers a security job. To do so, check the discipline product page under Content Type, Recommended Reading. To simplify security administration, we recommend that you run these jobs at the same time.

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, CHORGRP, and CHORTHD 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 ETJI095x*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.

Important! In the following content, CHORTSFB indicates the TSF Bridge started task; CHORNTSF indicates the TSF Server started task.

CHORTSFB

Started task name that is associated with the TSF Bridge.

CHORNTSF

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

CHORTSFR

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

CHORJBOS

Started task name that is associated with the CA Chorus Application 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

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 CA Chorus Application 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 security job that applies to your installation type and external security manager:
   a. For new installations, or for upgrades where you use a unique CA Chorus Administrator ID (CHORADM) for the Version 4.0 region:
      - CA ACF2: ETJI095A
      - CA Top Secret: ETJI095T
      - IBM RACF: ETJI095R

      Note: On CA Support Online, the links to the Version 4.0 security jobs are appended with two letters instead of one to differentiate these jobs from the Version 3.0 security jobs: ETJI095AC for CA ACF2, ETJI095TS for CA Top Secret, and ETJI095RA for IBM RACF.
   b. For Release 2.5 to Version 4.0 upgrades where you use the same CHORADM for the Release 2.5 and Version 4.0 regions and are using CA Top Secret:
      - CA Top Secret: ETJ2540T
      - If you are using CA ACF2 or IBM RACF, use the ETJI095x security job.
   c. For Version 3.0 to Version 4.0 upgrades where you use the same CHORADM for the Version 3.0 and Version 4.0 regions:
      - CA ACF2: ETJ3040A
      - CA Top Secret: ETJ3040T
      - IBM RACF: ETJ3040R
2. Review the entire job.
3. Edit the job according to the comments.
4. Submit the job.

   The noted security requirements are met.
5. (CA Top Secret only) Complete the following steps:
   a. 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 the security job.
   b. Restart CA Top Secret.

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.

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 the CA Chorus Application Server 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 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 Infrastructure Management for Networks and Systems**: CFAWZFS. The local path defaults to /cai/cetjr4m0/roles/performance. If you type /cai/dply/cetjr4m0/roles for the remote path, CA CSM creates the following path on the remote system: /cai/dply/cetjr4m0/roles/performance.
      - **For CA Chorus for Security and Compliance Management**: CE1MZFS. The local path defaults to /cai/cetjr4m0/roles/security. If you enter /cai/dply/cetjr4m0/roles for the remote path, CA CSM creates the following path on the remote system: /cai/dply/cetjr4m0/roles/security.
      - **For CA Chorus for Storage Management**: CE4HZFS. The local path defaults to /cai/cetjr4m0/roles/storage. If you type /cai/dply/cetjr4m0/roles for the remote path, CA CSM creates the following path on the remote system: /cai/dply/cetjr4m0/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 Configure Your Product using CA CSM (see page 69).

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 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 78).

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.
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) Bridge library)
      - *custom_hlq*.CC2DPLD (Includes the TSF Bridge product load library)
      - *custom_hlq*.CETJPLD (Includes the CA Chorus library)

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

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

```
SETPROG APF,ADD,DSNAME=custom_hlq.CC2DLOAD,<SMS|volume=volume>
SETPROG APF,ADD,DSNAME=custom_hlq.CC2DPLD,<SMS|volume=volume>
SETPROG APF,ADD,DSNAME=custom_hlq.CETJPLD,<SMS|volume=volume>
```

volume

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

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

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

g. ETJI0115 member in *custom_hlq*.CETJJCL (Configures the TSF datasource)

h. Copy customized CHORNTSF and CHORTSFB from CETJJCL to PROCLIB.

i. Start the TSF Bridge:

Note: If you are installing CA Chorus to use only the Software Development Kit, you do not need to start the TSF Bridge.

```
S CHORTSFB
```

A message indicating that the TSF Bridge is initialized is logged.

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

j. Start the TSF Server:

```
S CHORNTSF
```

A message indicating that the TSF Server is initialized is logged.

```
ETJTS001I *** TSF SERVER STARTUP COMPLETE ***
```

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

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

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

n. (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).

o. (Optional) If you are using an SMTP server to send notification emails, submit ETJI0135 from *custom_hlq*.CETJJCL.

p. (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 4 detail the jobs to submit for each discipline. Complete the applicable steps and then go to step 5.

CA Chorus Infrastructure Management for Networks and Systems Job Submission

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

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

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

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

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

CA Chorus for Security and Compliance Management Job Submission

3. 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

4. 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

5. 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 the CA Chorus Application Server 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 the CA Chorus Application Server startup is complete:

   ```
   ETJTC001I CA Chorus Startup Complete
   ```

6. Complete the tasks in Verify the Installation and Configuration (see page 78) and Post Installation Considerations (see page 80).

   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 CA Chorus Application Server host name and port in the URL using *one* of the following formats:

   `http://`*`chorusapplicationserverhostname`*`:`*`httpconnectorport`*`/Chorus`
   `https://`*`chorusapplicationserverhostname`*`:`*`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.

   chorusapplicationserverhostname

   Host name of the system where the CA Chorus Application Server is running. Use the value of the TEIID_MACHINE environment variable in CETJOPTN(ENVETJ).

   httpconnectorport

   Port number that is used to access the 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.

   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: 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: 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:

Note: This procedure applies only to disciplines that are using the TSF Bridge configuration.

- 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*.