

# CA Chorus™ Infrastructure Management for Networks and Systems

## Site Preparation Guide

Version 03.0.00, Seventh Edition



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

## CA Technologies Product References

This document references the following CA Technologies products:

- CA ACF2™ for z/OS (CA ACF2)
- CA Chorus™
- CA Chorus™ for DB2 Database Management
- CA Chorus™ Infrastructure Management for Networks and Systems (CA Chorus Infrastructure Management)
- CA Chorus™ Software Manager™ (CA Chorus Software Manager)
- CA Common Services
- CA Insight™ Database Performance Monitor for DB2 for z/OS (CA Insight DPM)
- CA NetMaster® NM for TCP/IP (CA NetMaster NM for TCP/IP)
- CA SYSVIEW® Performance Management (CA SYSVIEW)
- CA SYSVIEW® Performance Management Option for CICS (CA SYSVIEW Option for CICS)
- CA SYSVIEW® Performance Management Option for IMS (CA SYSVIEW Option for IMS)
- CA SYSVIEW® Performance Management Option for WebSphere MQ (CA SYSVIEW Option for WebSphere MQ)
- CA Top Secret® for z/OS (CA Top Secret)

# 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](mailto: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 list details the changes made since the sixth edition of this guide:

[Configure the CA SYSVIEW Data Source](#) (see page 32)—Added an optional step to activate the IMS DC Monitor.

[Addressing Security Requirements](#) (see page 25)—Updated the topics to cater for the FAWI095x security jobs, which helps you address the security requirements.

The following list details the changes made since the fifth edition of this guide:

[System Requirements](#) (see page 21)—Removed the target and distribution libraries.

How to Activate PassTicket Support for CA NetMaster NM for TCP/IP—Recommended using CHORWEBS as the APPL value to simplify PassTicket configuration.

The following list details the changes made since the fourth edition of this guide:

[Server Requirements](#) (see page 21)—Noted the new feature to automatically configure heap memory.

The following list details the changes made since the third edition of this guide:

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

[CA Chorus Infrastructure Management Architecture](#) (see page 9)—Added this topic.

Software Requirements—Clarified the FIXCAT label for back-end product maintenance.

Review the Systems External Security Product Requirements—Added authorization requirements for CHORTHD.

How to Activate PassTicket Support for CA NetMaster NM for TCP/IP—For Fix RO61896, updated the APPL value as the region primary VTAM ACB name when RAPPL is *not* specified.

[Configure the CA NetMaster NM for TCP/IP Data Source](#) (see page 31)—Added information about how to feed data to two TSF instances.

[Configure the CA SYSVIEW Data Source](#) (see page 32)—Added a note about multiple SYSVIEW suffixes.

The following list details the changes made since the second edition of this guide:

How to Activate PassTicket Support for CA NetMaster NM for TCP/IP—Corrected the APPL value as the region job name when RAPPL is not specified.

The following list details the changes made since the first edition of this guide:

[System Requirements](#) (see page 21)—Removed the heap memory requirements and added a specialty processor recommendation.

[Server Requirements](#) (see page 21)—Updated the heap memory requirements, noted the parameters to modify the heap size, noted that the values represent real storage, and moved the heap memory requirements to this new topic.

Software Requirements—Clarified browser support.

# Contents

---

## **Chapter 1: Architecture and Installation Overview 9**

CA Chorus Infrastructure Management Architecture .....	9
How the Installation Process Works.....	10
Network Data Source Setup Overview .....	14
Systems Data Source Setup Overview.....	16
DB2 Data Source Setup Overview .....	17

## **Chapter 2: Addressing General Prerequisites 19**

Software Requirements .....	19
Server Requirements.....	21
System Requirements .....	21
Port Requirements .....	22
Common Services Requirements .....	23
LMP Key Requirements .....	23

## **Chapter 3: Addressing Security Requirements 25**

Installer Security Privileges .....	25
Configure Data Source Requirements .....	26
Run the CA Chorus Infrastructure Management Discipline Security Jobs .....	27

## **Chapter 4: Configuring the Data Sources 29**

How to Configure the Data Sources .....	29
Review Configuration Prerequisites.....	30
Configure the CA NetMaster NM for TCP/IP Data Source .....	31
Configure the CA SYSVIEW Data Source.....	32
Configure the CA Insight DPM Data Source .....	35

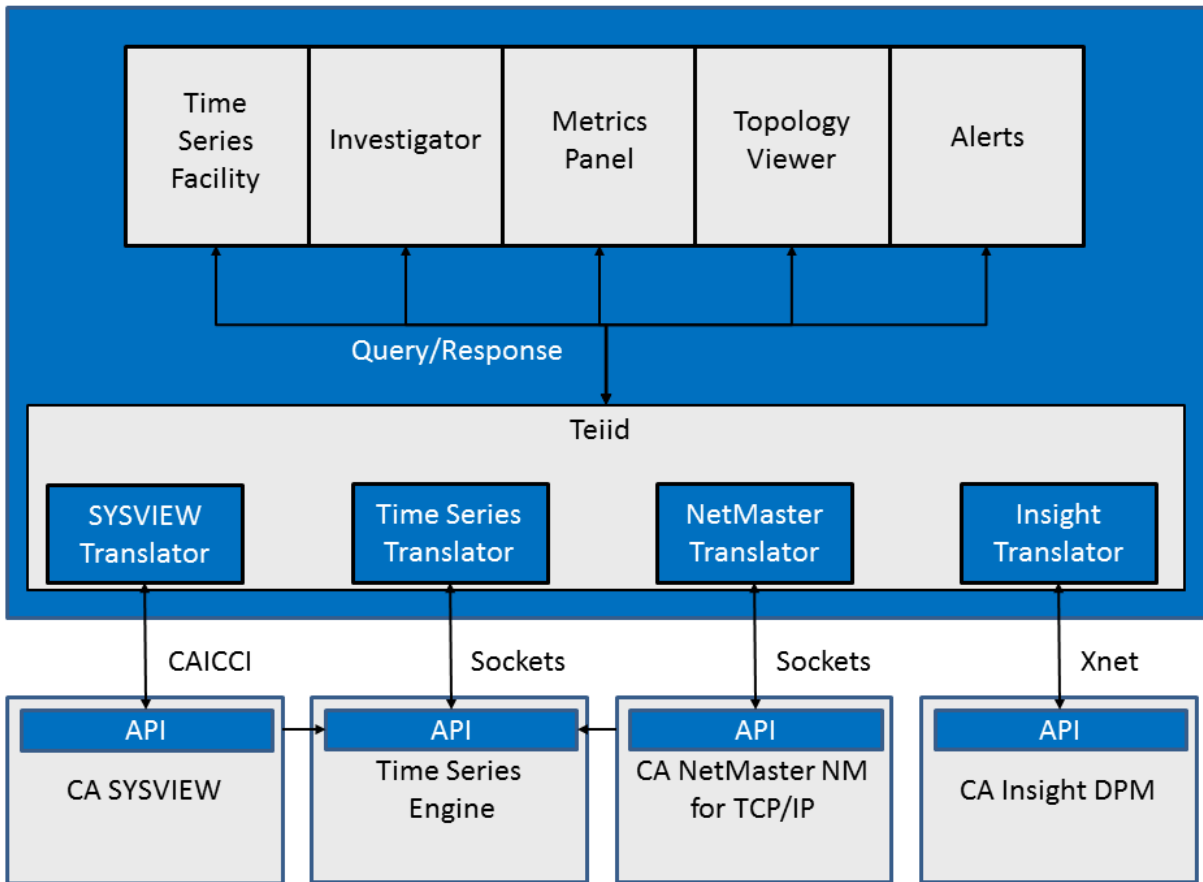


# Chapter 1: Architecture and Installation Overview

## CA Chorus Infrastructure Management Architecture

Using CA Chorus Infrastructure Management, you can analyze the z/OS system and network performance from a single interface.

The following diagram details the architecture and data flow for CA Chorus Infrastructure Management components:



The following list details the components and products that you use with CA Chorus Infrastructure Management:

**CAICCI**

Is a CA Common Services service that provides a software communications layer. CA SYSVIEW uses this layer to pass data to CA Chorus.

**Xnet**

Provides a communications subsystem for [set the idpm variable for your book]. Xnet (Execution Manager Networking) executes as a started task in its own address space. [set the idpm variable for your book] uses this subsystem to pass data to CA Chorus.

**[set the idpm variable for your book]**

Lets you monitor the DB2 activity and performance.

**CA NetMaster NM for TCP/IP**

Lets you monitor the network activity and performance.

**CA SYSVIEW**

Lets you monitor the system activity and performance.

**Teiid**

Is a data virtualization system that allows CA Chorus to use data from multiple, heterogeneous data stores through translators.

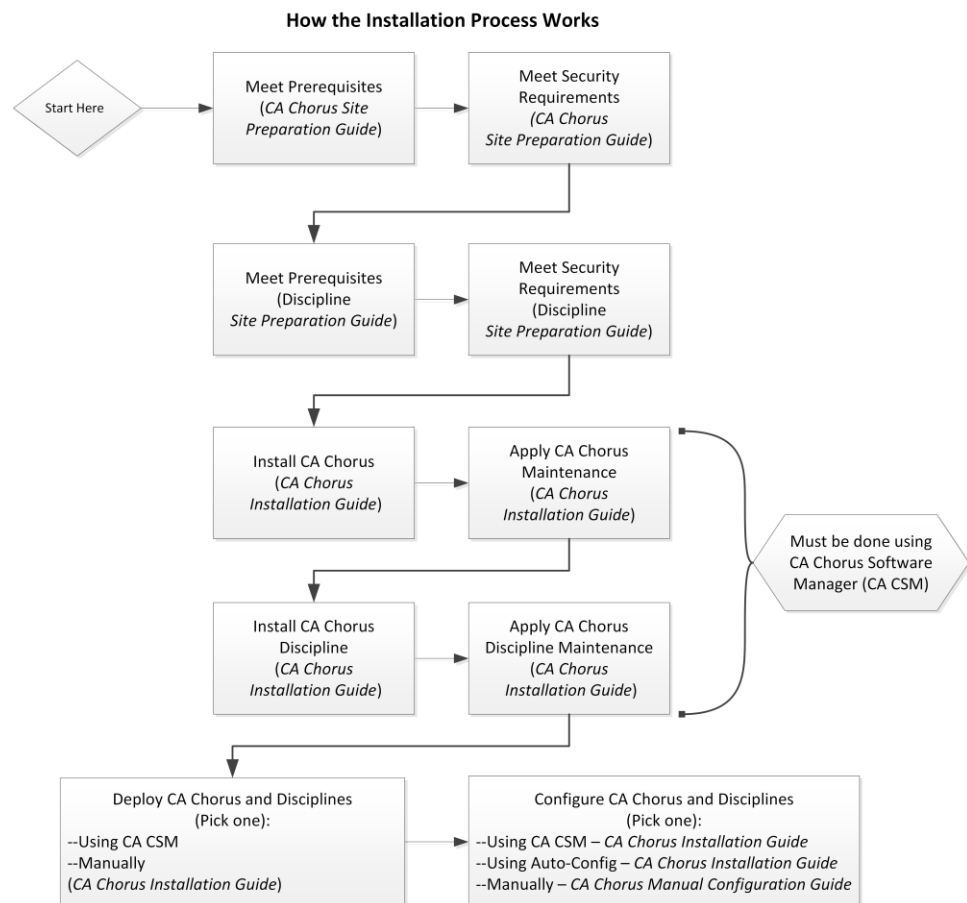
## How the Installation Process Works

This guide details the tasks that a system programmer and security administrator can complete before starting the installation, deployment, and configuration tasks that are described in the *Installation Guide*. The following diagram provides a high-level overview of the CA Chorus and discipline installation, deployment, and configuration process and the guides that you use.

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

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

**Note:** For the boxes that indicate work from the discipline *Site Preparation Guide*, repeat this step for each discipline that you are installing.



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

1. Meet the software, system, port, and other prerequisites as described in the *CA Chorus Site Preparation Guide*.
2. Meet the security requirements as described in the *CA Chorus Site Preparation Guide*.
3. Use the Prerequisite Validator to confirm that you have set up your system correctly as described in the *CA Chorus Site Preparation Guide*.

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

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

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

**Important!** To use the CA Chorus Software Manager Software Configuration Service, CA Chorus Software Manager deployment is required.

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

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

#### **CA CSM**

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

The *Installation Guide* includes the CA Chorus and discipline steps for this method.

#### **Automated Configuration**

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

The *Installation Guide* includes the CA Chorus and discipline steps for this method.

#### **Manual**

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

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

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

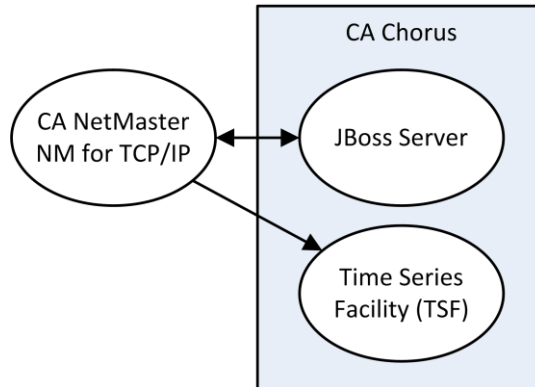
## Network Data Source Setup Overview

The following diagrams provide an overview of the network data source setup for CA Chorus Infrastructure Management. Your source of network data comes from one or more CA NetMaster NM for TCP/IP regions. On each system for which you want to monitor network data, you have a CA NetMaster NM for TCP/IP region running. For performance reasons, we recommend that CA Chorus and the CA NetMaster NM for TCP/IP region with which CA Chorus directly communicates be on the same system.

- Monitoring a single system only:

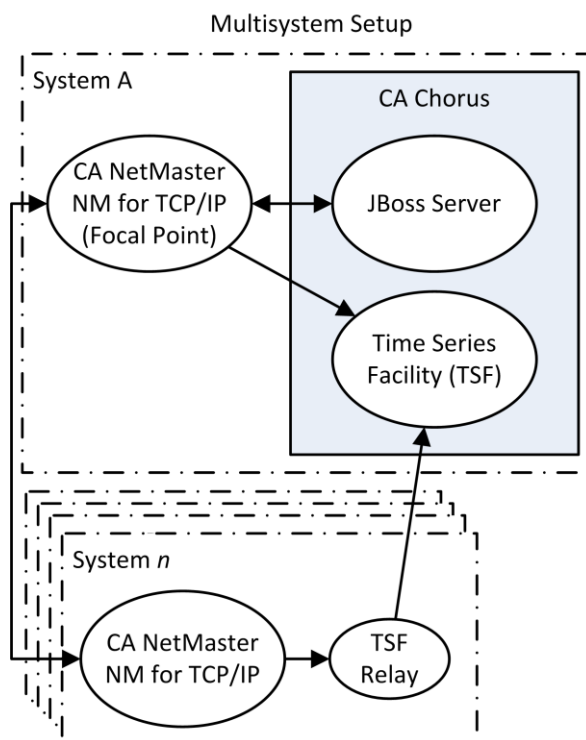
In this environment, your network data comes from a single CA NetMaster NM for TCP/IP region.

Single System Setup



- Monitoring multiple systems:

In this environment, your network data comes from linked CA NetMaster NM for TCP/IP regions. Set up communication between CA Chorus and a CA NetMaster NM for TCP/IP region that is a focal point. A focal point region sees the data in all linked regions. CA Chorus sends requests to one focal point region to retrieve data from the different systems.

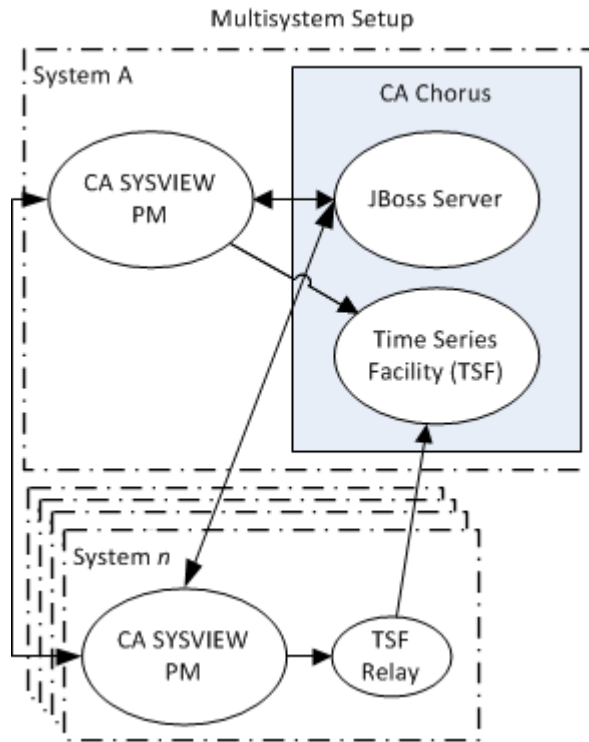


In either environment, CA Chorus requests data from one CA NetMaster NM for TCP/IP region through the JBoss server. Each CA NetMaster NM for TCP/IP region also sends performance metric data to Time Series Facility (TSF).

The CA NetMaster NM for TCP/IP region to which CA Chorus sends requests requires PassTicket support. CA Chorus uses PassTickets to let performance analysts access CA NetMaster NM for TCP/IP functions without having to log in manually. To support PassTicket, the region must use a security exit that specifies the RACROUTE APPL parameter.

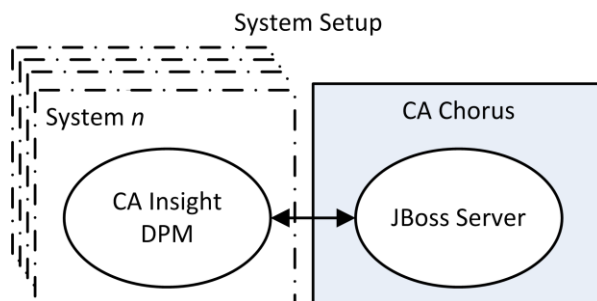
## Systems Data Source Setup Overview

The following diagram provides an overview of the systems data source setup for CA Chorus Infrastructure Management. Your source of data comes directly from one or more CA SYSVIEW instances. On each system for which you want to monitor system data, you have CA SYSVIEW running.



## DB2 Data Source Setup Overview

The following diagram provides an overview of the DB2 data source setup for CA Chorus Infrastructure Management. Your source of data comes directly from one or more CA Insight DPM instances. On each system for which you want to monitor DB2 data, you have CA Insight DPM running.





# Chapter 2: Addressing General Prerequisites

---

This section contains the following topics:

- [Software Requirements](#) (see page 19)
- [Server Requirements](#) (see page 21)
- [System Requirements](#) (see page 21)
- [Port Requirements](#) (see page 22)
- [Common Services Requirements](#) (see page 23)
- [LMP Key Requirements](#) (see page 23)

## Software Requirements

The following software is required for CA Chorus Infrastructure Management:

- CA Chorus Software—The following software is required:

- CA Chorus Version 03.0.00

For initial site installations, you install CA Chorus and the disciplines at the same time as described in the *CA Chorus Installation Guide*.

When you are installing a discipline into an existing CA Chorus instance, confirm that the version of your discipline matches the CA Chorus version.

- (Optional) CA Chorus for DB2 Database Management Version 03.0.00

**Note:** You require this software only if you run IBM DB2.

**Important!** This software is required to view DB2 performance data from CA Chorus Infrastructure Management. This guide describes the CA Chorus for DB2 Database Management prerequisites for this implementation. You do *not* have to refer to the *CA Chorus for DB2 Database Management Site Preparation Guide*.

If you are installing and configuring both CA Chorus for DB2 Database Management and CA Chorus Infrastructure Management, configure CA Chorus for DB2 Database Management first and no additional configuration is required for CA Chorus Infrastructure Management.

- The following software that provides the source of data:

**Important!** Apply all current CA Chorus FIXCAT maintenance for the CA Technologies products. The FIXCAT label is CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.\*, where \* indicates the version of CA Chorus that you are installing.

- (Optional) CA Insight DPM Version 15.0 or higher

**Important!** This software is required to view DB2 performance data from CA Chorus Infrastructure Management. If you have already installed CA Insight DPM while implementing CA Chorus for DB2 Database Management, no additional configuration is required for CA Chorus Infrastructure Management.

**Note:** For more information about installing CA Insight DPM, see the CA Database Management Solutions for DB2 for z/OS *Installation Guide* and *Implementation Guide*. To prepare CA Insight DPM for CA Chorus, see [Configure the CA Insight DPM Data Source](#) (see page 35) in this guide.

- CA NetMaster NM for TCP/IP Release 12.1

When you apply the maintenance, pay attention to the following fixes:

- R056668 has HOLDDATA reason ACTION (also replaces fix R055386).
- R056669 has HOLDDATA reason ACTION and DDDEF (also replaces R055387). Apply R056669 DDDEF HOLDDATA before SMP/E RECEIVE is done.

**Note:** For more information about preparing the CA NetMaster NM for TCP/IP region for CA Chorus, see [How to Configure the Data Sources](#) (see page 29) in this guide.

- CA SYSVIEW Performance Management Release 13.7 with the following site applicable options:

- CA SYSVIEW Option for CICS
- CA SYSVIEW Option for IMS
- CA SYSVIEW Options for WebSphere MQ

**Note:** For more information about installing and configuring these products, see the product installation and implementation documentation. To prepare CA SYSVIEW for CA Chorus, see [Configure the CA SYSVIEW Data Source](#) (see page 32) in this guide.

- (Optional) IBM DB2 V8 New Function Mode (NFM), or DB2 9, or DB2 10

**Note:** This software is required to view DB2 performance data from CA Chorus Infrastructure Management.

- PC software that is required for each user:
  - Adobe Flash Player 9.0.124 or above
  - At the release of Version 3.0, CA Chorus supports Microsoft Windows Internet Explorer 9 and Mozilla Firefox 13 through 19. As new browsers are released, we will validate them and post compatibility on the [CA Chorus product page](#) under Content Type, Recommended Reading.  
**Note:** CA Chorus requires a minimum screen resolution of 1024 x 768. If your screen resolution does not meet this requirement, use full screen mode (F11 in most browsers) to include the scroll bar on the display.
  - The browser must be enabled for Java.

## Server Requirements

Confirm that your site meets the following requirements:

### Real Storage

200 MB for CA Chorus Infrastructure Management plus the additional 2450 MB of heap memory for CA Chorus.

200 MB of additional heap memory is required for CA Chorus for DB2 Database Management.

**Note:** CA Chorus automatically configures the heap memory size based on the disciplines that you install at JBoss startup.

**Note:** If all disciplines are installed, 3150 MB is required. CA Chorus automatically configures the heap memory size based on the disciplines that you install. This configuration is done during the CA CSM Software Configuration Service (SCS) or in CETJJCL(ETJI0150).

## System Requirements

Confirm that your site addresses the following requirements:

### Disk

CA Chorus Infrastructure Management requires approximately 30 cylinders on the zFS that holds the pax installation file.

**Note:** This space can be reclaimed after installation.

CA Chorus for DB2 Database Management requires 251 tracks.

### Processor

CA Chorus uses a JavaVM environment on z/OS. So, we *strongly* recommend that you use a zIIP specialty processor for the best performance and better use of resources.

## Port Requirements

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

### **Xnet port (for CA Insight DPM)**

Specifies the TCP/IP port number that the listener process in the Xnet (execution manager networking) communications server uses. This one-way Xnet port is required for CA Chorus for DB2 Database Management. The PORT symbolic parameter in the PXNPROC JCL identifies this parameter value and is typically customized during CA Insight DPM post-installation processing. When Xnet is started, it binds the specified port number to a listening socket and it accepts connections from CA Chorus clients.

CA Chorus for DB2 Database Management provides the data source handler (DSH) component that runs in the JBoss server. The DSH makes connections to the Xnet ports on behalf of CA Chorus clients. The Xnet port number is specified in the DSH db2tools.cfg configuration file to define the Xnet servers to the DSH.

Each Xnet server that you are running requires a PORT specification and a corresponding connection definition in the db2tools.cfg file. To update the db2tools.cfg file, use E3KCFG10 in *your\_chorusdba\_hlq.CE3KPARAM*. Specify the PORT value in *your\_chorusdba\_hlq.CE3KPARAM(E3KCFG10)*.

### **Server port (for CA NetMaster NM for TCP/IP)**

Is the port that the region uses to accept CA Chorus requests. The CHORUS parameter group in the region identifies this port.

### **More information:**

[Configure the CA NetMaster NM for TCP/IP Data Source](#) (see page 31)

[Configure the CA Insight DPM Data Source](#) (see page 35)

## Common Services Requirements

The following CA Common Services for z/OS (CCS) are used with CA Chorus Infrastructure Management:

- CAICCI
- CA LMP

**Note:** These services are delivered and installed with CA Common Services for z/OS. If other CA Technologies products are installed at your site, these services could be installed. If these services have not been installed, do so now. For more information about the installation and configuration of these components, see the CCS documentation.

Additional common services can be used with the products that must be installed to support CA Chorus Infrastructure Management.

**Note:** For more information about those requirements, see the related product installation and implementation documentation.

## LMP Key Requirements

The CA License Management Program (CA LMP) tracks licensed software in a standardized and automated way. CA LMP reports on activities that are related to the license, usage, and financials of CA Technologies products.

CA Chorus and its disciplines are licensed with an LMP key. You acquire the LMP key with one of the following methods:

- From your product media
- From CA Support

During startup, CA Chorus Infrastructure Management license validation is performed by calling the CA LMP service of the CAIRIM component. CAIRIM is a component of CA Common Services for z/OS. The CAIRIM component verifies the product LMP keys. When a CA Chorus user logs in, the CA Chorus server makes LMP checks against the appropriate product keys. For example, if CA Chorus for Storage Management and CA Chorus Infrastructure Management are installed, the LMP check is performed for both disciplines, and the seat count for these disciplines is increased.

To report on and to verify compliance with CA Technologies product seat license concurrent usage, SMF type 89 records are collected over the required reporting period. A registered software usage report can be produced from the SMF type 89 records using the IBM z/OS product usage report utility program, IFAURP. The IFAURP report utility supports specification of a software vendor such that only CA products are included in the generated reports. Use member CHSMFRPT in *your\_chorus\_hlq*.CETJJCL to extract SMF type 89 records from the installation SMF collection data sets. After submission, this job sorts the extracted records and produces the software usage reports.

**Note:** For more information about CA LMP, CAIRIM, and generating software product registration reports, see the CA Common Services for z/OS documentation.

# Chapter 3: Addressing Security Requirements

---

This section contains the following topics:

[Installer Security Privileges](#) (see page 25)

[Configure Data Source Requirements](#) (see page 26)

[Run the CA Chorus Infrastructure Management Discipline Security Jobs](#) (see page 27)

## Installer Security Privileges

Before you begin the installation process, verify that the CA Chorus Infrastructure Management installer user ID has the following security privileges defined:

- For UNIX System Services:
  - (Optional) Ability to manipulate zFS data sets. This ability requires UPDATE authority to the appropriate entities within the FSACCESS class. Commented out by default.
    - FSACCESS lets you secure access to a ZFS file system container (that is, a data set). The resource name is the ZFS file system name.
    - For example, if you defined a ZFS file system named OMVS.ZFS.WEBSRV.TOOLS and then created directories U1 and U2 with files in the directories, a resource check for class FSACCESS resource OMVS.ZFS.WEBSRV.TOOLS would occur when a user tries to access a file in directory U1 or U2 in the ZFS file system. For more details, see the applicable security product documentation.
  - A valid OMVS definition and the installer user ID has a valid UID that is *not* UID(0).
  - Superuser authority.
  - READ access to the following resources in the FACILITY class:
    - (Optional) BPX.SUPERUSER
    - (Optional) BPX.FILEATTR.APF
    - (Optional) BPX.FILEATTR.PROGCTL
    - (Optional) BPX.FILEATTR.SHARELIB
    - (Optional) BPX.SERVER
    - SUPERUSER.FILESYS.PFSCTL profile in UNIXPRIV resource class
    - GROUP (GID) installation group (Default: CHORGRP)

- For z/OS:
  - Authority to create, update, and execute from the installation data sets and libraries.
  - Authority to execute the commands to manipulate the external security manager (CA ACF2, CA Top Secret, or IBM RACF) database.
- For DB2, SYSADM authority is required to execute DB2 catalog and product customization tasks for CA Insight DPM.

## Configure Data Source Requirements

To authorize CA Chorus Infrastructure Management users to work with the data sources, complete the following tasks.

**Note:** If you have already completed a task as part of configuring a different CA Chorus discipline, you do *not* have to redefine it for this discipline.

**Follow these steps:**

1. If CA NetMaster NM for TCP/IP has *not* previously used PassTicket, then update the RAPPL SXCTL parameter in the CA NetMaster NM for TCP/IP region as CHORWEBS. Otherwise, if CA NetMaster NM for TCP/IP has previously used PassTicket or CHORWEBS is *not* a suitable value, then use a [FAWI095x security job](#) (see page 27) to activate PassTicket support.

When using PassTicket, the CA NetMaster NM for TCP/IP region identifies itself to the security systems, CA ACF2, CA Top Secret, or IBM RACF, with the application ID of *applid*. The region must use a security exit that specifies the RACROUTE APPL parameter. *applid* is the value of that parameter.

CHORWEBS is the default application ID for which PassTickets are generated for CA Chorus users.

**Note:** For more information about CHORWEBS and PassTicket, see *CA Chorus Site Preparation Guide*.

The region *must not* specify SEC=NO in TESTEXEC(RUNSYSIN). If you use the distributed security exit (for example, SEC=NMSAF), the RAPPL SXCTL parameter specifies the APPL value. The default is the primary VTAM ACB name of the region (PRI value in RUNSYSIN).

- The NMDRVCTL DD statement in the region started task identifies the RUNSYSIN member.
- The DD=SXCTL command in RUNSYSIN allocates the data set member that specifies the SXCTL parameters.

**Note:** For more information, see the *CA Mainframe Network Management Security Guide*.

2. Define the users as network operators in the CA NetMaster NM for TCP/IP region to which CA Chorus sends requests. These definitions include the CA Chorus ancillary user ID (default CHORTHU).

If the region specifies SEC=NMSAF and the region uses the MODEL user facility, configure the following SXCTL parameter: **WEBMODEL=YES**.

3. To view DB2 subsystem data from CA Chorus Infrastructure Management, the users require EXECUTE authority on the CA Insight DPM product plans.

**Note:** For more information about using the Product Authorizations Facility to assign this right, see the *CA Database Management Solutions for DB2 for z/OS General Facilities Reference Guide*.

## Run the CA Chorus Infrastructure Management Discipline Security Jobs

The FAWI095x security jobs consolidate the security requirements (user, started task, and PassTicket) for the CA Chorus Infrastructure Management discipline. These jobs authorize users to work in the discipline and address other security requirements.

If you want to use CA Chorus Infrastructure Management to monitor DB2 subsystem performance, use an E3KI095x job to define extra security:

- If you do *not* have CA Chorus for DB2 Database Management, use the job to define the extra security.
- If you have CA Chorus for DB2 Database Management, use the job to define security for any users who do *not* yet have access to the DB2 subsystem data.

### Follow these steps:

1. Log in to CA Support Online, and go to the CA Chorus Infrastructure Management product page.
2. Go to Content Type, Recommended Reading, and download the appropriate security jobs:
  - FAWI095A for CA ACF2
  - FAWI095T for CA Top Secret
  - FAWI095R for IBM RACF
  - (Optional) E3KI095A for CA ACF2
  - (Optional) E3KI095T for CA Top Secret
  - (Optional) E3KI095R for IBM RACF
3. Customize the jobs for your environment as described within the JCL, and save your changes.

4. Submit the jobs.

The expected return code is zero.

5. Review the output of the jobs for verification that the security definitions have been defined successfully.

# Chapter 4: Configuring the Data Sources

---

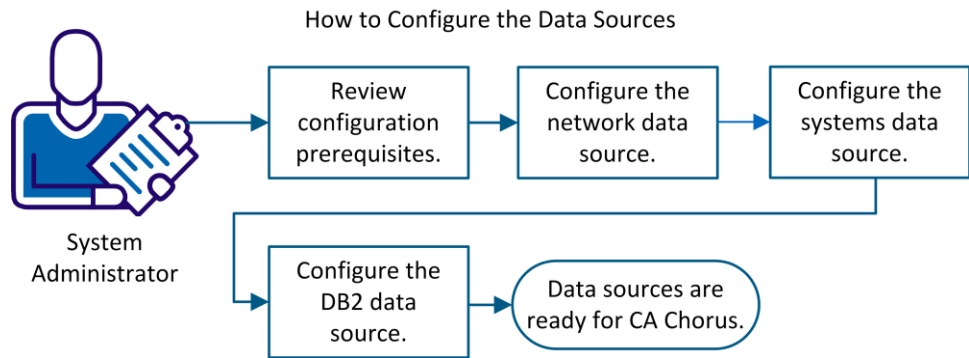
These topics describe how to configure the network, systems, and DB2 data sources.

## How to Configure the Data Sources

As the system administrator, you want to configure the network, systems, and DB2 data sources for CA Chorus. The performance analysts use this data to monitor the health of the network, systems and DB2, and isolate performance problems.

You use CA NetMaster NM for TCP/IP as the source of the network data; you use CA SYSVIEW as the source of the systems data; you use CA Insight DPM as the source of DB2 performance data.

The following illustration provides an overview of the process:



The process has the following tasks:

1. [Review configuration prerequisites](#) (see page 30).
2. [Configure the network data source](#) (see page 31).
3. [Configure the systems data source](#) (see page 32).
4. [Configure the DB2 data source](#) (see page 35).

At the end of the process, the network, systems, and DB2 data sources are ready to communicate with CA Chorus.

## Review Configuration Prerequisites

Before you start, determine the systems for which you want to monitor data.

Review the following configuration requirements:

- On each of the systems from which you want to access data, you have configured the appropriate data collecting software:
  - CA NetMaster NM for TCP/IP region
  - CA SYSVIEW
  - CA Insight DPM
- (CA NetMaster NM for TCP/IP) If you have multiple regions, you have linked the regions. We recommend that you have CA Chorus and a focal point region on the same system. A focal point region sees the data in all linked regions. CA Chorus sends requests to one focal point region to retrieve data from the different systems.

**Important!** CA Chorus can send requests to only one CA NetMaster NM for TCP/IP region.

- (CA NetMaster NM for TCP/IP) The focal point region *must* not specify SEC=NO in TESTEXEC(RUNSYSIN). Use, for example, SEC=NMSAF.
- (CA NetMaster NM for TCP/IP) You have configured the WEBCENTER parameter group in the focal point region for the web interface port.
- (CA NetMaster NM for TCP/IP) You are a defined administrator in the regions.

## Configure the CA NetMaster NM for TCP/IP Data Source

To prepare the connections to CA Chorus, configure the CA NetMaster NM for TCP/IP regions through the CHORUS parameter group.

### Follow these steps:

1. Log on to the focal point region to which CA Chorus sends requests.

The Primary Menu panel appears. The panel contains the IP address of the region. Record this IP address:

IP address = \_\_\_\_\_

2. Enter the **/PARMS** panel shortcut.
3. Enter **U** next to the CHORUS parameter group:

**Note:** For information about the fields, press F1 (Help).

- In the Allow Connections? field, specify **YES**.
- In the TSF Suffix field, specify **PROD**.
- Leave the TSF Registration Library field blank.

A typical region configuration puts the region load library, CC2DLOAD, in a JCL STEPLIB, and you do not have to complete this field. If the region does *not* use STEPLIB, specify the fully qualified library name in this field (for example, *your\_netmaster\_hlq.CC2DLOAD*).

- Record the port number in the Server Port field: \_\_\_\_\_.

4. Press F6 (Action) and then F3 (File).
5. (Optional) In a multisystem environment, log on to, and update the CHORUS parameter group for, each of the other linked regions:

- In the Allow Connections? field, specify **NO**.
- In the TSF Suffix field, specify **PROD**.
- Leave the TSF Registration Library field blank.

A typical region configuration puts the region load library, CC2DLOAD, in a JCL STEPLIB, and you do not have to complete this field. If the region does *not* use STEPLIB, specify the fully qualified library name in this field (for example, *your\_netmaster\_hlq.CC2DLOAD*).

After you update the group, press F6 (Action) and then F3 (File) to apply and save the changes.

**Important!** If the TESTEXEC(RUNSYSIN) member in a region specifies the INFILE parameter, the region starts up using an initialization file. Regenerate this file for subsequent startups. For more information, see the *CA NetMaster Network Management for TCP/IP Administration Guide*.

**Note:** If you require a region to feed data to two TSF instances, add the following statement in the TESTEXEC(NMINIT) member: `$GLBL $TSFOVRL = tsf_suffix1,tsf_suffix2` (for example, `$GLBL $TSFOVRL = PROD,A`).

You have configured the regions for CA Chorus. You have also recorded the following values that are required when you configure the discipline as described in *CA Chorus Installation Guide*:

- IP address of the focal point region
- Region server port number

After you configure CA Chorus Infrastructure Management and start the data flow, CA Chorus can request network data on demand, and can receive network metrics and alerts.

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

## Configure the CA SYSVIEW Data Source

As the system administrator, you want CA Chorus to provide systems data to the performance analysts. The analysts use this data to monitor and isolate performance problems.

CA SYSVIEW is the source of this data. You configure CA SYSVIEW on each LPAR to enable the following functions:

- Enable CA Chorus to request system data from CA SYSVIEW.
- Enable CA SYSVIEW to send system data to CA Chorus.

**Follow these steps:**

1. Access the system configuration options member GSVXGSVX that is located in the CNM4BSAM SMP/E target system parameter library data set (the IPL concatenation).

```
SYSVIEW.BASE.PARMLIB(GSVXGSVX)  
system.parmLib(GSVXGSVX)
```

The system configuration options member sets configuration options during the CA SYSVIEW initialization.

2. Change the following configuration options to yes in the member GSVXGSVX:

```
Option-Chorus=yes
```

```
Option-MVS=Yes
```

**Yes**

Activates the CA Chorus Infrastructure Management integration and enables CA SYSVIEW data flow to CA Chorus Infrastructure Management.

**No**

Prevents CA Chorus Infrastructure Management integration.

**Default: No**

3. (Optional) Change the following configuration options to yes in the member GSVXGSVX:

```
Option-CICS=yes
```

```
Option-IMS=yes
```

```
Option-WebSphereMQ=yes
```

**Yes**

Activates the CA Chorus Infrastructure Management integration and enables data flow for those CA SYSVIEW options to CA Chorus Infrastructure Management.

**No**

Prevents CA Chorus Infrastructure Management integration.

**Default: No**

The data flow to CA Chorus Infrastructure Management is enabled.

CA Chorus Infrastructure Management can request and receive system data from CA SYSVIEW.

4. (Optional) Open the SYSVIEW parmlib member TSF and edit the member to change the following Time Series Facility default values. The parameters in the member TSF control the sending of data to TSF. Only change the default values when the defaults do not apply to your site.

**Note:** The Chorus complex contains one TSF Server address space. The other systems in the Chorus complex run a TSF Relay address space. CA SYSVIEW communicates with a TSF address space (Relay or Server) through TCP/IP on the local system running CA SYSVIEW.

- TSF-Hostname - localhost

Change the TSF-Hostname parameter when *localhost* is not the local host name.

- TSF-IPVersion - IPV4

Possible values are IPV4 and IPV6. Change the TSF-IPVersion parameter when you are using IPV6.

- TSF-Region-ID - \*

Only change the TSF Region-ID if the TSF installer changed the default value of the TSF parameter TSFSUFFIX. The TSF-Region-ID parameter must match the TSFSUFFIX specification.

**Note:** For multiple suffixes with CA SYSVIEW, you need the multiple instances for CA SYSVIEW.

When the TSF installation is complete, the SYSVIEW TSFLIST command displays the local TSF address space and the associated Region ID.

Data flow to CA Chorus Infrastructure Management Time Series Facility is enabled.

5. (Optional) Activate the IMS DC Monitor.

This step is only necessary to display the wait delay values for the IMS Transaction Times objects in Investigator. The other IMS objects and modules do not require the DC Monitor to be active.

  - a. Open the CA SYSVIEW IMSLOGR parmlib member.
  - b. Set the ACTIVATE-DC-MONITOR option to Yes.
6. Review the CA SYSVIEW installation member INST0003 in the sysview.SAMPJCL data set to ensure the z/FS release dependent file systems are mounted and permanently available.

## Configure the CA Insight DPM Data Source

**Note:** If your site already has installed and configured the CA Chorus for DB2 Database Management discipline, no additional configuration is needed.

As the application administrator, you want CA Chorus to provide DB2 performance data to the performance analysts. The analysts use this data to monitor and isolate DB2 performance problems.

CA Insight DPM is the source of this data. You configure CA Insight DPM on each LPAR to enable the following functions:

- Enable CA Chorus to request DB2 performance data from CA Insight DPM.
- Enable CA Insight DPM to send DB2 performance data to CA Chorus.

**Follow these steps:**

1. Update the Xnet configuration in the CA Database Management Solutions for DB2 for z/OS:

- a. To enable PassTicket support, insert the following line before or after the CMD entries in the *your\_db2tools\_hlq.CDBAPARM(PXNPARM)*:

```
PASSNAME (DB2T00LS)
```

DB2TOOLS is the default application ID. This value must match the application ID value that was specified during the security PassTicket configuration.

- b. Update the Xnet started task procedure in *your\_db2tools\_hlq.CDBASAMP(PXNPROC)* to set the following parameters:

- Port
- TCP
- XMANID

**Note:** If you are using an Xmanager value of 0000 in the PTXMAN started task procedure, update the XMANID parameter to the release version. For example, specify XMANID=1600 if you are running Version 16.0 of the CA Database Management Solutions for DB2 for z/OS.

- c. Restart each Xnet by entering the following command:

```
S PXNPROC
```

A message indicates that the Xnet started task has initialized successfully.

**Note:** For more information about Xmanager and Xnet, see the *CA Database Management Solutions for DB2 for z/OS General Facilities Reference Guide*.

2. Specify XNETAGT=YES in the CA Insight DPM data collector initialization parameters for each DB2 subsystem in your CA Chorus configuration. The data collector initialization parameters reside in *your\_db2tools\_hlq.SOURCE(IDDCPRMS)*.

**Note:** For more information about the XNETAGT parameter and initializing CA Insight DPM data collectors, see the *CA Insight DPM System Reference Guide*.