CA Chorus™ for Security and Compliance Management

Site Preparation Guide

Version 04.0.00, Third Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA ACF2™ (CA ACF2)
- CA ACF2™ Option for DB2
- CA Chorus
- CA Chorus for Security and Compliance Management
- CA Chorus Software Manager™ (CA CSM)
- CA Common Services for DB2 for z/OS (CA Common Services)
- CA Compliance Manager for z/OS (CA Compliance Manager)
- CA Datacom/AD® (CA Datacom/AD)
- CA Datacom® Server (CA Datacom Server)
- CA Distributed Security Interface for z/OS (CA DSI Server)
- CA LDAP Server (CA LDAP Server)
- CA Top Secret® for z/OS (CA Top Secret)
- CA Top Secret® Option for DB2

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 second edition of this documentation:

- Set Up Workload Manager (WLM) and Resource Recovery Attach Facility (RRSAF) (see page 105)—Noted that the WLM NUMTCB value should be between 20 and 40.
- Link the DB2 Modules into Functions (see page 106)—Updated the topic for the CIA4LNK1 job.
- Unified Install Process Overview (see page 21)—Updated the overview for clarity.

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

- Software Requirements (see page 53)—Noted that you should disable pop-up blockers for your browser before you access your CA Chorus instance.

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

- Unified Install Process (see page 21)—This chapter provides direction on using the unified install process to unload and configure the security discipline software prerequisites as a single set.
- Server Requirements (see page 57)—Noted that CA Chorus now automatically configures the heap memory size.

Contents

Chapter 7: Implementing CIA Real-Time for CA Chorus for Security and Compliance Management 95

Chapter 1: Architecture and Installation Overview

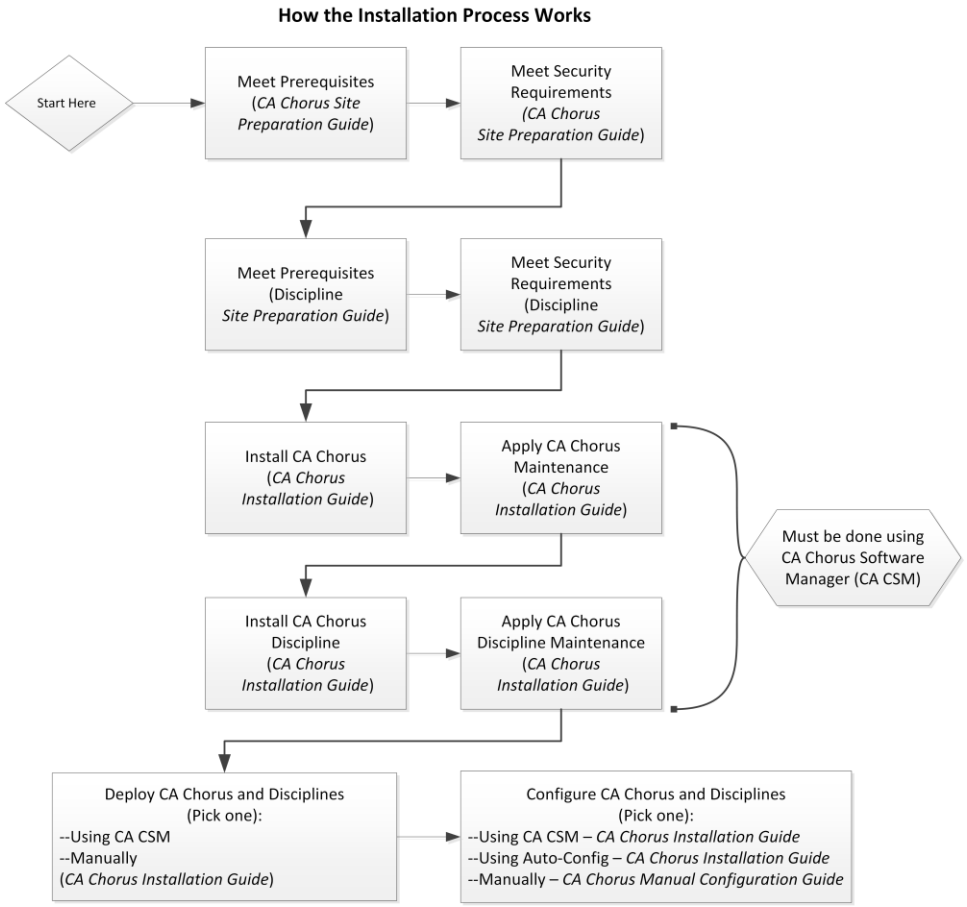
How the Installation Process Works

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 CSM 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 untailored.

7. Deploy CA Chorus and the applicable disciplines using CA CSM or a manual process. The *CA Chorus Installation Guide* details both methods.

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

   Important! For deployments from CA CSM, 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 CSM Software Configuration Service, CA CSM deployment is required.

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

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

   CA CSM

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

   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.

Installation Methods

The CA Chorus for Security and Compliance Management discipline can be installed using an automated or manual process.

Unified Installation

Unloads and configures the security discipline software prerequisites as a single set. The unified method simplifies and expedites the installation process. At this time, the unified method supports CA Datacom/AD on a single system. If you wish to install on multiple systems or want to use DB2 as your database, use the manual method. To install the CA Chorus for Security and Compliance Management discipline using the automated method see Unified Install Process (see page 21).

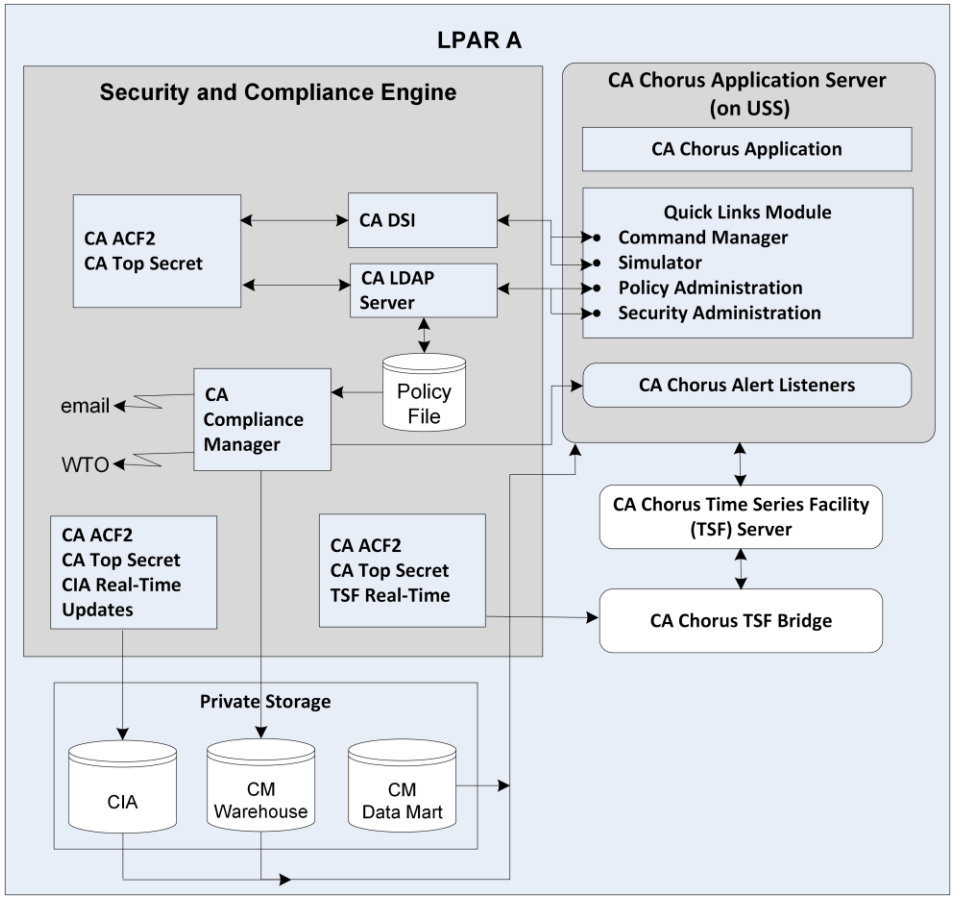
Manual Installation

Manually steps you through the unloading and configuration of the security software prerequisites. The manual method supports CA Datacom/AD and DB2 and lets you install on multiple systems. You can also select specific components of CA Compliance Manager such as Alerts or Logger. To install the CA Chorus for Security and Compliance Management discipline using the manual method, see Addressing General Prerequisites for Manual Installation.

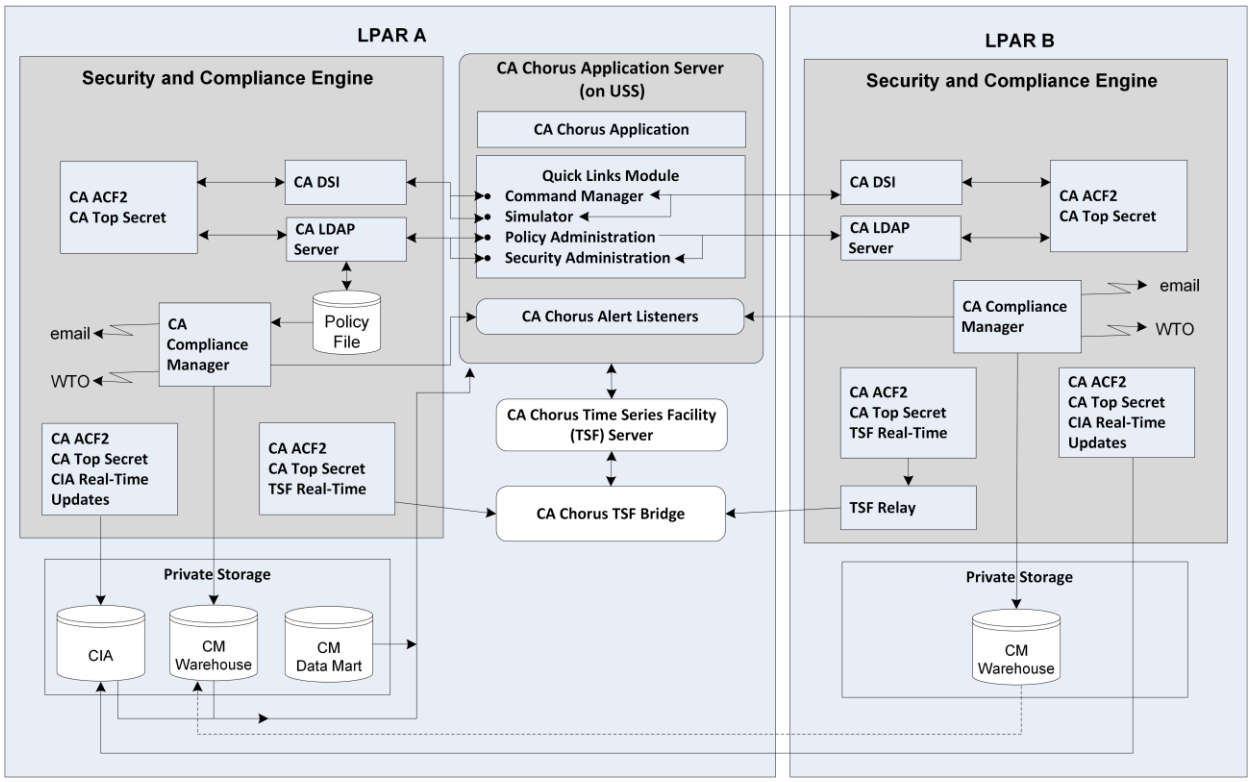
Architecture

The following diagrams provide an overview of the CA Chorus for Security and Compliance Management discipline architecture. After installation and setup, use it to manage security resources across your z/OS enterprise.

- Single LPAR architecture:



- Multiple LPAR architecture:



Observe the following:

- In the single LPAR architecture it is common to have the security engine and CA Chorus Application Server in the same LPAR, but this setup is not required.
- The multiple LPAR architecture and setup diagram shows two LPARs. You can have more LPARs if needed.

To install and configure this discipline you must:

- Install and configure the security engine components on one or more selected LPARs.
- Install and configure a single CA Chorus instance to communicate with the security engines.

The diagrams illustrate the basic architecture:

LPARs

Identify logical partitions of a mainframe (z/OS system), on which you execute your External Security Manager (ESM) as a back-end engine for this discipline. Multiple LPARs are supported.

CA Chorus Application Server

Contains the CA Chorus system. Includes the following components:

CA Chorus Application

Provides the browser support and components to communicate with the back-end engines for the various disciplines, such as the security engine.

Quick Links Module

For this discipline this module includes the Administer Compliance Policy, Administer Security Definitions, and Simulate Access Attempt interfaces.

Security Command Manager Module

Issues native commands to backend security engines from the CA Chorus interface.

CA Chorus Listeners

Provides the service for receiving Alerts sent by the various backend security engines.

CA Chorus Time Series Facility (TSF)

Provides the facility for receiving, storing, and querying metrics about objects managed by the security backend engines. Because all metrics are date- and time-stamped, a series can be graphed over time to show trends, and to project into the future.

Security Engines

Composite of the ESM and compliance products that together provide the input to this discipline. Includes but is not limited to CA ACF2, CA Top Secret, CA Compliance Manager, and CA LDAP Server.

Shared Storage

Represents all storage devices that are shared across the CA Chorus disciplines.

Private Storage

Represents storage devices that are shared only across this discipline.

Chapter 2: Unified Install Process

Unified Install Process Overview

The unified install process installs and configures the software that is required to implement CA Chorus for Security and Compliance Management as a single set. Doing so simplifies and expedites the install process. The unified method supports CA Datacom/AD on a single LPAR only. The unified install does not support installing subsets of the products or components.

- To install CA Chorus for Security and Compliance Management on multiple LPARs, you must perform the entire unified install process on each LPAR *or* use the manual install method.
- To install CA Chorus for Security and Compliance Management using IBM DB2 as your repository, you must use the manual install method.

The following steps are required to complete the unified install process:

- Form Pre-Installation Planning Team (see page 22)
- Review Unified Software Prerequisites (see page 22)
- Review Installer Security Privileges (see page 25)
- Setting Up a File System for the Pax Files (see page 26)
- Acquire the Unified Install Process Pax Files (see page 29)
- Create a Product Directory from the Pax File (see page 34)
- Copy Installation Files to z/OS Data Sets (see page 37)
- Import an SMP/E Environment to CA CSM (Optional) (see page 39)
- Apply Preventative Maintenance (see page 40)
- Run the Staging Jobs (see page 41)
- Customize Members (see page 42)
- Clean Up the USS Directory (Optional) (see page 44)

Note: For a detailed list of started tasks (STCs) and their start and stop order, see the STC Reference (see page 207)topic.

Form Pre-Installation Planning Team

The CA Chorus Security and Compliance Discipline installation is a detailed process that requires personnel in several areas of expertise. We suggest that you meet with each of the following team members before the installation begins and review the roles of each person:

- Systems programmer for z/OS
- Storage administrator for DASD allocations
- Security administrator for access permissions and security configuration
- Database administrator for DB2 and/or CA Datacom/AD configuration

For this meeting, we recommend that you refer to the platform and discipline *Site Preparation Guide* and *Installation Guide*.

Additionally, given the scope of the installation, we recommend that team members review the entire guide before beginning the installation.

Important! Do not begin the installation until all team members have a clear understanding of their installation responsibilities. Failure to do so can impact your ability to complete the installation in a timely manner.

Review Unified Install Process Software Prerequisites

The following software is required when installing CA Chorus for Security and Compliance Management using the unified install process. To verify that the software with the latest maintenance has been installed, contact your installer.

Note: For more information about installing and configuring these products, see the product installation and implementation documentation for the associated product.

- CA ACF2 r15, CA Top Secret r15, or IBM RACF Version 1 Release 13 with current maintenance. For information about current CA Technologies product maintenance, see http://ca.com/support.
- Support for IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0 Service Release 5 or 7 (5655-W44), including optional JZOS batch launcher.

Note:

- As part of pre-installation planning, you determine if you are implementing Compliance Information Analysis (CIA) for CA Chorus and if so, if you are using a CA Datacom/AD or DB2 CIA repository.
- The CA Chorus LMP key must be available on every z/OS image where the CIA real-time feature is enabled.

  The CA Compliance Manager LMP key must be available on every z/OS image where IBM RACF is installed. When the IBM RACF unload utility is executed, the utility performs an LMP check. Without the key, the RACF unload utility cannot be used.

Unified Install Process Worksheet

Use the following worksheet to record variable values for referencing during the unified installed process. The first table can be used to fill in the values for your site. The second table indicates which jobs and data sets contain the variables.

Variable	Value
instlib_hlq	
yourUSSpaxdirectory	
yourUSSinstalldirectory	
yourjavahome	
stagelib_hlq	
stagelib_vol	
custlib_hlq	
config_hlq	
your_javalib	
your_tcpdata	
HLQ	
MLQ	
VOL	

ESM_LINKLIB	
ESM_DDTRLIB	
CCSLOADLIB	
CIA_MUF_HOMEPATH	
CMGR_HOMEPATH	
HOST_ADDRESS	

Variable	**unzipjcl**	**updcsi**	**STAG4DC***	**RUNCONF**	**CONFIG.DATA**
instlib_hlq	X	X	X		
yourUSSpaxdirectory	X				
yourUSSinstalldirectory	X	X		X	X
yourjavahome	X	X		X	
yourclasspath	X				
stagelib_hlq			X	X	
stagelib_vol			X		
custlib_hlq				X	
config_hlq				X	
your_javalib				X	
your_tcpdata				X	X
HLQ					X
MLQ					X
VOL					X
ESM_LINKLIB					X
ESM_DDTRLIB					X
CCSLOADLIB					X
CIA_MUF_HOMEPATH					X
CMGR_HOMEPATH					X
HOST_ADDRESS					X

Review Installer Security Privileges

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

- For UNIX System Services:
  - A valid OMVS definition and the installer user ID have a valid UID that is *not* UID(0).
  - Superuser authority.
  - READ access to the following resources in the FACILITY class:
    - (Optional) BPX.SUPERUSER
    - BPX.FILEATTR.APF
    - BPX.FILEATTR.PROGCTL
    - BPX.FILEATTR.SHARELIB
    - (Optional) BPX.SERVER
    - SUPERUSER.FILESYS.PFSCTL profile in UNIXPRIV resource class

    (Optional, depending on your site's security configuration) Ability to manipulate zFS data sets. This requires UPDATE authority to the appropriate entities within the FSACCESS class.

    Note: Verify with your Security Administrator if FSACCESS permissions are needed.

    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: You defined a zFS file system that is named OMVS.ZFS.WEBSRV.TOOLS, and then you created directories U1 and U2 with files in the directories. A resource check for class FSACCESS resource OMVS.ZFS.WEBSRV.TOOLS occurs 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.
- For z/OS:
  - Authority to read, create, update, and execute from the CA Chorus Security and Compliance Discipline installation data sets and libraries.
  - Authority to execute commands to manipulate the external security manager (CA ACF2, CA Top Secret, or IBM RACF) database.
  - APF-authorization and other security requirements that must be performed through an external security product are defined during the CA Chorus configuration process, as described in the *CA Chorus Installation Guide.* You complete those tasks during the installation because you need to access various jobs and members from the installation package.

Setting Up a File System for the Pax File

The product installation process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system that is dedicated to the product acquisition and create the directory in this file system.

Allocate and Mount a File System

The following provides an overview of the allocating and mounting a file system process. The steps to perform this task are available following this overview.

You need a UNIX System Services (USS) directory and a file system with adequate space to perform the following tasks:

- Receive product pax files from http://ca.com/support.
- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.

We recommend that you allocate and mount a file system that is dedicated to Pax ESD. The amount of space that you need for the file system depends on the following variables:

- The size of the pax files that you intend to download.
- Whether you plan to keep the pax files after unpacking them. We do not recommend this practice.

We recommend that you use one directory for downloading and unpacking pax files. Reusing the same directory minimizes USS setup. You need to complete the USS setup only one time. You can reuse the same directory for subsequent downloads. Alternatively, you can create a directory for each pax download.

Important! Downloading pax files for the SMP/E installation as part of the Pax ESD process requires write authority to the UNIX System Services (USS) directories that are used for the Pax ESD process. In the file system that contains the Pax ESD directories, you also need free space approximately 3.5 times the pax file size to download the pax file and unpack its contents. For example, to download and unpack a 14 MB pax file, you need approximately 49 MB of free space in the file system hosting your Pax ESD directory.

You can use the zSeries File System (zFS) or hierarchical file system (HFS) for product downloads.

This procedure describes how to perform the following tasks:

- Allocate a zFS or an HFS.
- Create a mount point in an existing maintenance USS directory of your choice.

- Mount the file system on the newly created mount point.

  Note: You must have either SUPERUSER authority, or the required SAF profile setting to allow you to issue the USS mount command for the file system.

  Important! For new zFS, allocate and mount appropriate resource class FSACCESS authority must be granted to the LDAP4SRV (CA LDAP Server) and DSI4SRV (CA DSI Server for CIA Real-Time) started task which access the new zFS file.

- Optionally, permit write access to anyone in the same group as the person who created the directory.

  Important! USS commands are case-sensitive.

Follow these steps:

1. Allocate the file system by customizing one of the following samples to your site requirements.

   - On a zFS, use the following sample:

```
//DEFINE   EXEC PGM=IDCAMS
//SYSPRINT DD   SYSOUT=*
//SYSUDUMP DD   SYSOUT=*
//AMSDUMP  DD   SYSOUT=*
//SYSIN    DD *
  DEFINE CLUSTER ( +
  NAME(your_zFS_data_set_name) +
  STORAGECLASS(class) +
  LINEAR +
  CYL(primary secondary) +
  SHAREOPTIONS(3,3) +
  )
/*
//FORMAT   EXEC PGM=IOEAGFMT,REGION=0M,
// PARM=('-aggregate your_zFS_data_set_name -compat')
//SYSPRINT DD   SYSOUT=*
//SYSUDUMP DD   SYSOUT=*
//STDOUT   DD   SYSOUT=*
//STDERR   DD   SYSOUT=*
//CEEDUMP  DD   SYSOUT=*
//*
```

- On an HFS, use the following sample:

```
//ALCHFS EXEC PGM=IEFBR14
//CAPAX  DD   DSN=your_HFS_data_set_name,
//            DISP=(NEW,CATLG,DELETE),UNIT=3390,
//            DSNTYPE=HFS,SPACE=(CYL,(primary,secondary,1))
```

The file system is allocated.

Note: Ensure that the zFS or HFS data set name that you use conforms to your data set naming conventions for USS file systems. If the allocation of the file system data set fails, it is because of environmental settings not allowing for the allocation. On an HFS, try using the ISPF 3.2 Data Set Utility to allocate your HFS data set.

2. Create a mount point for the file system. This example shows how to create a /CA/CAPAX directory in an existing directory, /u/maint. From the TSO OMVS shell, enter the following commands:

```
cd /u/maint/
mkdir CA
cd CA
mkdir CAPAX
```

Note: This document refers to this structure as *yourUSSpaxdirectory*.

The mount point is created.

3. Mount the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
MOUNT FILESYSTEM('your_zFS_data_set_name')
      MOUNTPOINT('yourUSSpaxdirectory')
      TYPE(ZFS)  MODE(RDWR)
      PARM(AGGRGROW)
```

- On an HFS, use the following sample:

```
MOUNT FILESYSTEM('your_HFS_data_set_name')
      MOUNTPOINT('yourUSSpaxdirectory')
      TYPE(HFS)  MODE(RDWR)
```

The file system is mounted.

4. (Optional) Set security permissions for the directory. You can use the chmod command to let other users access the Pax ESD directory and its files. For example, to allow write access to the Pax ESD directory for other users in your USS group, from the TSO OMVS shell, enter the following command:

```
chmod -R 775 /yourUSSpaxdirectory/
```

Write access is granted.

Note: For more information about the chmod command, see the IBM *z/OS UNIX System Services User Guide* (SA22-7802).

Acquire the Unified Install Process Pax Files

To begin the CA Technologies product installation procedure, copy the product pax file into the USS directory that you set up.

Important! Downloading pax files for the SMP/E installation as part of the Pax ESD process requires write authority to the UNIX System Services (USS) directories that are used for the Pax ESD process. Also, you must have available USS file space before you start the procedures in this guide.

Use one of the following methods:

- Download the product pax file from http://ca.com/support to your PC (see page 30), and then upload it to your USS file system.

  If you download a zip file, you must unzip it before uploading to your USS file system.
- Download the pax files from http://ca.com/support directly to your USS file system.
- Download the pax file from the product DVD to your PC, and then upload the pax files to your USS file system. (see page 33)

This section includes the following information:

- A sample batch job to download a product pax file from the CA Support Online FTP server directly to a USS directory on your z/OS system
- Sample commands to upload a pax file from your PC to a USS directory on your z/OS system

Important! The FTP procedures vary due to local firewall and other security settings. Consult your local network administrators to determine the appropriate FTP procedure to use at your site.

Ensure that sufficient free space is available in the USS file system that you are using to hold the product pax file. If you do not have sufficient free space, error messages similar to the following will appear:

```
EZA1490I Error writing to data set
EZA2606W File I/O error 133
```

When the download finishes, the pax file size in your USS directory matches the value in the Size column for the corresponding pax file on the CA Technologies Products Download window.

Download Files to a PC Using Pax ESD

You can download product installation files from http://ca.com/support to your PC.

Follow these steps:

1. Log in to http://ca.com/support, and click Download Center.

   The Download Center web page appears.

2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and gen level (if applicable), and click Go.

   The CA Product Download window appears.

3. Download an entire CA Technologies product software package or individual pax files to your PC. If you download a zip file, you must unzip it before continuing.

   Note: For traditional installation downloads, see the *Traditional ESD User Guide*. For information about download methods, see the Download Methods and Locations article. Go to http://ca.com/support, log in, and click Download Center. Links to the guide and the article appear under the Download Help heading.

Download Files Using Batch JCL

You download a pax file from http://ca.com/support by running batch JCL on the mainframe. Use the sample JCL, shown below and attached to the PDF file as CAtoMainframe.txt to perform the download.

Important! The PDF version of this guide includes sample JCL jobs that you can copy directly to the mainframe. To access these jobs, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click a file to view a sample JCL. We recommend that you use the latest version of Adobe Reader for viewing PDF files.

Note: We recommend that you follow the preferred download method as described on http://ca.com/support. This JCL procedure is our preferred download method for users who do not use CA CSM. We also include the procedure to download to the mainframe through a PC in the next section.

Example: CAtoMainframe.txt, JCL

The following text appears in the attached CAtoMainframe.txt JCL file:

```
//GETPAX   JOB (ACCOUNTNO),'FTP GET PAX ESD PACKAGE',
//          MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*********************************************************************
//* This sample job can be used to download a pax file directly from  *
//* CA Support Online to a USS directory on your z/OS system.         *
//*                                                                   *
//* When editing the JCL ensure that you do not have sequence numbers *
//* turned on.                                                        *
//*                                                                   *
//* This job must be customized as follows:                           *
//* 1. Supply a valid JOB statement.                                  *
//* 2. The SYSTCPD and SYSFTPD JCL DD statements in this JCL may be   *
//*    optional at your site. Remove the statements that are not      *
//*    required. For the required statements, update the data set     *
//*    names with the correct site-specific data set names.           *
//* 3. Replace "Host" based on the type of download method.           *
//* 4. Replace "YourEmailAddress" with your email address.            *
//* 5. Replace "yourUSSpaxdirectory" with the name of the USS         *
//*    directory used on your system for Pax ESD downloads.           *
//* 6. Replace "FTP Location" with the complete path                  *
//*    and name of the pax file obtained from the FTP location        *
//*    of the product download page.                                  *
//*********************************************************************
//GETPAX   EXEC PGM=FTP,PARM='(EXIT TIMEOUT 120',REGION=0M
//SYSTCPD  DD   DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSFTPD  DD   DSN=yourFTP.DATA.dataset,DISP=SHR
//SYSPRINT DD   SYSOUT=*
//OUTPUT   DD   SYSOUT=*
//INPUT    DD   *
Host
anonymous YourEmailAddress
lcd yourUSSpaxdirectory
binary
get FTP_location
quit
/*
```

Follow these steps:

1. Replace *ACCOUNTNO* with a valid JOB statement.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.

   The job points to your profile.

3. Replace *YourEmailAddress* with your email address.

   The job points to your email address.

4. Replace *yourUSSpaxdirectory* with the name of the USS directory that you use for Pax ESD downloads.

   The job points to your USS directory.

5. Locate the product component to download on the CA Support Product Download window.

   You have identified the product component to download.

6. Click Download for the applicable file.

   Note: For multiple downloads, add files to a cart.

   The Download Method window opens.

7. Click FTP Request.

   The Review Download Requests window displays any files that you have requested to download.

   Note: We send you an email when the file is ready to download or a link appears in this window when the file is available.

8. Select one of the following methods:

   Preferred FTP

   Uses CA Technologies worldwide content delivery network (CDN). If you cannot download using this method, review the security restrictions for servers that company employees can download from that are outside your corporate network.

   Host Name: ftp://ftpdownloads.ca.com

   Alternate FTP

   Uses the original download servers that are based on Long Island, New York.

   Host Name: ftp://scftpd.ca.com for product files and download cart files and ftp://ftp.ca.com for individual solution files.

   Both methods display the host, user name, password, and FTP location, which you then can copy into the sample JCL.

   Note: The following links provide details regarding FTP: the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

   Important! If your FTP commands are incorrect, it is possible for this job to fail and still return a zero condition code. Read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

   After you run the JCL job, the pax file resides in the mainframe USS directory that you supplied.

Download Files to Mainframe through a PC

You download the product installation files to your PC and transfer them to your USS system.

Follow these steps:

1. Download the product file to your PC using one of the following methods:

   - Pax ESD (see page 30). If you downloaded a zip file, first unzip the file to use the product pax files.
   - DVD. Copy the entire product software package (or individual pax files) to your PC.

   The pax file resides on your PC.

   Note: Do *not* change the format of the pax.Z.

2. Open a Windows command prompt.

   The command prompt appears.

3. Customize and enter the following FTP commands:

   ```
   FTP mainframe
   userid
   password
   bin
   lcd C:\PC\folder\for\thePAXfile
   cd /yourUSSpaxdirectory/
   put paxfile.pax.Z
   quit
   exit
   ```

   mainframe

   Specifies the z/OS system IP address or DNS name.

   userid

   Specifies your z/OS user ID.

   password

   Specifies your z/OS password.

C:*PCfolder**for**thePAXfile***

Specifies the location of the pax file on your PC.

Note: If you specify a location that has blanks or special characters in the path name, enclose that value in double quotation marks.

yourUSSpaxdirectory

Specifies the name of the USS directory that you use for Pax ESD downloads.

***paxfile*.pax.Z**

Specifies the name of the pax file to upload.

The pax file is transferred to the mainframe.

Create a Product Directory from the Pax File

You can submit a pax command or use the sample JCL (shown below or in the attached PDF file) to perform the following actions:

- Extracts the files and directories that are packaged within the pax file.
- Creates a USS directory in the same directory structure where the pax file resides.
- Automatically generates a product and level-specific directory name.

Submitting the Pax Command

Set the current working directory to the directory containing the pax file, and create a directory in your USS directory by entering the following command in OMVS or from a command prompt:

```
pax -rvf paxfile.pax.Z
```

Replace *paxfile.pax.Z* with the name of the actual pax file.

Using the Sample JCL

Use the sample JCL, shown below and in the attached PDF file, as Unpackage.txt to extract the product pax file into a product installation directory.

Important! The PDF version of this guide includes sample JCL jobs that you can copy directly to the mainframe. To access these jobs, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click a file to view a sample JCL. We recommend that you use the latest version of Adobe Reader for viewing PDF files.

Sample Unpackage.txt JCL

The following text appears in the attached Unpackage.txt JCL file:

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX ESD PACKAGE',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*********************************************************************
//* This sample job can be used to invoke the pax command to create   *
//* the product-specific installation directory.                      *
//*                                                                   *
//* This job must be customized as follows:                           *
//* 1. Supply a valid JOB statement.                                  *
//* 2. Replace "yourUSSpaxdirectory" with the name of the USS         *
//*    directory used on your system for Pax ESD downloads.           *
//* 3. Replace "paxfile.pax.Z" with the name of the pax file.         *
//* NOTE: If you continue the PARM= statement on a second line,       *
//*       start entering characters in column 16 and make sure        *
//*       the 'X' continuation character is in column 72.             *
//*********************************************************************
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSpaxdirectory/; pax -rvf paxfile.pax.Z'
//*UNPAXDIR EXEC PGM=BPXBATCH,
//* PARM='sh cd /yourUSSpaxdirectory/; pax                            X
//*             -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

Follow these steps:

1. Replace *ACCOUNTNO* with a valid JOB statement.
2. Replace *yourUSSpaxdirectory* with the name of the USS directory that you use for product downloads.

   The job points to your specific directory.
3. Replace *paxfile.pax.Z* with the name of the pax file.

   The job points to your specific pax file.
4. Submit the job.

   The job creates the product directory.

Note: If the PARM= statement exceeds 71 characters, uncomment and use the second form of UNPAXDIR instead. This sample job uses an X in column 72 to continue the PARM= parameters to a second line.

Example: JCL File, Unpackage.txt, to Customize

The following text appears in the attached Unpackage.txt JCL file:

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX ESD PACKAGE',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*********************************************************************
//* This sample job can be used to invoke the pax command to create   *
//* the product-specific installation directory.                      *
//*                                                                   *
//* This job must be customized as follows:                           *
//* 1. Supply a valid JOB statement.                                  *
//* 2. Replace "yourUSSpaxdirectory" with the name of the USS         *
//*    directory used on your system for Pax ESD downloads.           *
//* 3. Replace "paxfile.pax.Z" with the name of the pax file.         *
//* NOTE: If you continue the PARM= statement on a second line,       *
//*       start entering characters in column 16 and make sure        *
//*       the 'X' continuation character is in column 72.             *
//*********************************************************************
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSpaxdirectory/; pax -rvf paxfile.pax.Z'
//*UNPAXDIR EXEC PGM=BPXBATCH,
//* PARM='sh cd /yourUSSpaxdirectory/; pax                            X
//*             -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

Copy Installation Files to z/OS Data Sets

Use this procedure to invoke the SMP/E GIMUNZIP utility to create MVS data sets from the files in the product-specific directory.

The file UNZIPJCL in the product directory contains a sample job to GIMUNZIP the installation package. You edit and submit the UNZIPJCL job to create z/OS data sets.

Follow these steps:

1. Use ISPF EDIT or TSO ISHELL to edit the UNZIPJCL sample job. You can perform this step in one of the following ways:
   - Use ISPF EDIT. Specify the full path name of the UNZIPJCL file.
   - Use TSO ISHELL. Navigate to the UNZIPJCL file and use the E line command to edit the file.
2. Edit the job card to include a valid job class, MSGCLASS, and accounting information, according to your site's standards.
3. Change all occurrences of "<instlib_hlq>" to the high-level qualifier (HLQ) for z/OS data sets that the installation process uses.

   All occurrences of "<instlib_hlq>" are set to your high-level qualifier for z/OS data sets.
4. Change the "<yourUSSpaxdirectory>" to the product-specific directory created by the pax command.

   All occurrences of "<yourUSSpaxdirectory>" are set to the product-specific directory created by the pax command.
5. Change "<yourUSSinstalldirectory>" to the USS directory path where the USS files for CA Compliance Manager, CA LDAP, and CA Datacom are copied. This must be an existing path. Specify the entire path except for the trailing "/".
6. To use the default SMS class for interim files, leave volume="*" as is. To use a specific volser, change volume="*" to volume="packname". The files being downloaded are an entire SMP/E environment. We recommend that you specify a volume for permanent retention of the SMP/E environment.
7. If ICSF is not active, perform the following steps:
   a. Change the "<yourjavahome>" to your Java runtime directory. This directory varies from system to system.
   b. Perform one of the following steps:
      - Change the "<yourclasspath>" to your Java application classes directory, typically /usr/lpp/smp/classes/.
      - Change HASH=YES to HASH=NO on the GIMUNZIP parameter.

   One of the following occurs: ICSF is active or you are using Java.

8. Submit the UNZIPJCL job.
9. The UNZIPJCL job unloads all the target and DLIB libraries and associated CSI which contains the following products:
   - CA Compliance Manager
   - CA LDAP Server
   - CA DSI Server
   - CA Datacom/AD
   - CA Easytrieve

   The UNZIPJCL job completes with a zero return code. Messages GIM69158I and GIM48101I in the output and IKJ56228I in the JES log are acceptable.

   GIMUNZIP creates z/OS data sets with the high-level qualifier that you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed.

   Note: For more information, see the IBM *SMP/E for z/OS Reference (SA22-7772)*.
10. Update the CSI parameters and DDDEFs. The UPDCSI job in the SAMPJCL library created by the previous step updates the CSI parameters and DDDEFS to complete the SMP/E environment.
    - Change the JOB statement to conform to your site standards.
    - Change all occurrences of "<instlib_hlq>" to the same high level qualifier that was specified for “instlib_hlq” in the UNZIPJCL job.
    - Change "<yourUSSinstalldirectory>" to the USS directory path that was specified for "yourUSSinstalldirectory" in the UNZIPJCL job. Specify the entire path except for the trailing "/".
    - Change "<yourjavahome>" to the same path that was specified for "yourjavahome" in the UNZIPJCL job. Specify the entire path except for the trailing "/".
    - Change "<STORCLASS=STRCLS>" to specify valid SMS information or valid volume information for your system.
11. Run the UPDCSI job.

Import an SMP/E Environment to CA CSM (Optional)

Future maintenance for the CA Chorus for Security and Compliance Management can be applied using SMP/E or CA CSM. This procedure steps you through applying maintenance using CA CSM. You can use CA CSM to maintain products that were installed previously using SMP/E by placing the relevant SMP/E environments under CA CSM management. A wizard is available to guide you through the process.

Some zones of the migrated SMP/E environment can have missing or partially populated DDDEF entries. CA CSM requires DDDEFs to maintain previously installed products successfully. For those SMP/E environment zones, you obtain the missing DDDEFs from the original product SMP/E installation JCL during SMP/E environment migration. This JCL is the member that is used to install the SMP/E product using the receive or apply and accept functions.

Note: We recommend that you use your product installation JCL when migrating an SMP/E environment to ensure product SMP/E environment integrity.

Follow these steps:

1. From the SMP/E Environments tab, click the Migrate SMP/E Environment link in the Actions section.

   You are prompted to identify the SMP/E environment.

2. Define a meaningful name for the environment. Specify the data set name of the SMP/E environment you want to migrate, and click Next.

   The functions in the SMP/E environment are listed.

3. Review the information and select Next.

   A list of zones with DDDEF associations appears.

4. (Optional) Review and update the DDDEFs obtained from JCL for each zone individually:

   - Click Manage DDDEFs for the zone whose DDDEFs you want to review individually.

     A pop-up window displays a list of DDDEFs for the zone.

   - Review the list of DDDEFs and select (to add to a zone) or clear (to remove from a zone) the corresponding check boxes.

     Note: If some DDDEFs from the list cannot be added to the zone or they exist in the zone, the corresponding check boxes are disabled. You cannot select the DDDEFs from the list.

   - Click Close to save changes and return to the wizard.

5. Click Next.

   If any file systems mounted to the path specified in the DDDEFs are found, a list of the file systems is displayed.

6. Review the file systems.

   Zones of the migrated SMP/E environment are listed.

   Note: Only the existing zones and the zones to which you have access appear.

7. Click next

   Verify a prefix for each zone and click Next. Prefixes are only used as HLQ defaults during future base installations into the same SMP/E environment. If necessary, these defaults can be overridden during the base installation.

   A list of advanced settings appears.

8. Add SMP/E Environment to Working Set

   Adds the migrated SMP/E environment to your working set. A working set is a selected group of SMP/E environments which you want to work. Future displayed information is based on the working set. For example, maintenance information is shown. The information is not shown for environments outside the set.

9. Click Next.

   The summary page appears.

10. Review the information and click Migrate.

A dialog that shows the progress of the task opens. When the task completes, you can click Show Results on the Progress tab to close this dialog. The task output browser opens and you can view the action details. Click Close to close the task output browser.

Note: You can perform other work while a task is in progress. Click Hide to exit the dialog and view the task status later on the Tasks tab.

After the migration is successfully completed, information about the SMP/E environment and associated products is saved in the CA CSM database. The migrated environment appears on the tree in the SMP/E Environments section on the left side.

Apply Preventative Maintenance

Obtain any maintenance released for the FMIDs you just installed using CA CSM or your site's normal maintenance procedures. Contact your systems programmer for assistance.

Run the Staging Jobs

The staging jobs copy the required job, procedure, parameter, and configuration members from the installation libraries into staging libraries. The staging jobs can be found in the LDAP JCL library (<instlib_hlq>.CHRSEC.LDAP.CDT9JCL) created by the previous steps. Choose the appropriate staging job for your system:

STAG4DCA
: Copies members needed for CA ACF2 systems installing components compatible with CA Chorus v4.0. Uses role-based rules for the security administration jobs.

STAG4DCU
: Copies members needed for CA ACF2 systems installing components compatible with CA Chorus v4.0. Uses UIDSTRING-based rules for the security administration jobs.

  Note: The security administration jobs contain UIDSTRING-based rules that require manual edits during the customization phase of the process. All manual steps are described in the AREADME file and in the jobs themselves.

STAG4DCT
: Copies members needed for CA Top Secret systems installing components compatible with CA Chorus v4.0.

STAG4DCR
: Copies members needed for RACF systems installing components compatible with CA Chorus v4.0.

Follow these steps:

1. Modify the job card according to site standards.
2. Edit the following variables:

   INSTLIB_HLQ

   HLQ of the libraries that were created when the unified install process ESD file was installed. This value must match the value that was used for the “instlib_hlq” variable in the UNZIPJCL job

   STAGELIB_HLQ

   HLQ of the libraries that will be created by this job to hold copies of all members needed for the configuration process. It is acceptable to use the same value for all of the high level qualifiers.

   STAGELIB_VOL

   Volume used for stage libraries. If using SMS, replace the 'VOL=SER=STAGELIB_VOL' statement with the appropriate SMS statement.

   STAGELIB_UNIT

   Unit used for stage libraries.
3. Run the staging job.

   The staging libraries are created.

Customize Members

The RUNCONF job executes a customization program that edits the members in the staging libraries. This program must be executed twice. The first run allocates a data set and copies all the variables that are required to customize the members. The second run substitutes the values specified for the variables into the members. To customize the members for your environment, complete the following steps.

Follow these steps:

1. Edit the RUNCONF job in the <stagelib_hlq>.CHRSEC40.STAGE.JOBLIB staging library created in the previous step:
   - Edit the JOB statement to conform to your site standards.
   - Change "<yourUSSinstalldirectory>" to the complete USS path for the LDAP directory that was created during the UNZIPJCL job. Do not specify the trailing slash.
   - Change "<your_javalib>" to the fully qualified name of the data set containing your IBM Java modules.
   - Change "<your_tcpdata>" to the fully qualified data set name of the z/OS TCP/IP .DATA file.
   - Change "<yourjavahome>" to the complete USS path for the java JDK.
   - Change "<stagelib_hlq>" to the value that was specified for stagelib_hlq in the stag4*xxx* job.
   - Change "<config_hlq>" to the high level qualifier you wish to use for the data set that is allocated to hold your customization variables. It is acceptable to use the same value for all of the high level qualifiers.
   - Change "<custlib_hlq>" to the high level qualifier you wish to use for the customized libraries. It is acceptable to use the same value for all of the high level qualifiers.

   Note: Additional values can optionally be changed. See the notes in RUNCONF for more information.
2. Run the RUNCONF job.

   The first run allocates the <config_hlq>.CHRSEC40.CONFIG.DATA data set. All required variables are copied into this data set.
3. Review and edit the <config_hlq>.CHRSEC40.CONFIG.DATA (referred to as CONFIG.DATA later) data set. Several variables require changes and more variables can be changed, if necessary, to conform to site standards. See the documentation in this member to determine which variables require modification, which can optionally be changed, and which should not be modified.

You must review or update the variables in the CONFIG.DATA data set prior to running the RUNCONF job for the second time. If a default value is provided, ensure that it is correct for your site. Variables with a value of 'changeme' must be modified.

4. Run the RUNCONF job again. The second run copies all members from the staging libraries into the customized libraries and applies all customizations to the members.

5. Review the customized jobs in the <custlib_hlq>.CHRSEC40.CUST.JOBLIB, procedures, parameter members, and configuration members in the customized libraries.

   Note: If any values require changes, it is recommended that you edit the value in the CONFIG.DATA data set and rerun the RUNCONF job. Doing so ensures that the change is propagated to all members that need the value.

6. Print and review the AREADME member in the customization JOBLIB data set for more instructions and notes regarding the customized members. To ensure this process is successful, you must follow the additional instructions contained within the AREADME.

   Important! We recommend printing the AREADME member for reference while editing and running the customized jobs.

7. Run the customized jobs that now reside in the customization <custlib_hlq>.CHRSEC40.CUST.JOBLIB. The jobs use the following naming conventions:

   - The first character of the job is J.
   - The second through sixth characters indicate the sequence number for the member. The jobs *must* be run in this order.

   The jobs must be run in the correct order using the sequence number.

   Most jobs are expected to get a return code of 0. See the AREADME file for exceptions. If a job does not have a return code of 0, review the job output.

   Note: the jobs ending in "SA" are security administration jobs. Some of these jobs require manual intervention in order to match your site standards and run successfully. Detailed instructions for these steps are provided in the AREADME member and in the comment boxes inside the jobs. Please review these jobs with the appropriate security administrator for correctness.

8. Some members created by this process are started task procedures and parameter files. Several customized jobs copy these members into PROCLIB and PARMLIB libraries. See the AREADME file for the data set names for these libraries. You are required to copy the procedures into a system proclib before you can start any of the started tasks. The parameter and config libraries are specified in several of these procedures. If you move the parameter members, you must also edit the procedures to specify the new libraries and ensure that the tasks have access to the new libraries.

9. Start the started tasks in the order described in the AREADME file. Ensure each started task starts successfully.

Note: After successfully starting the started tasks described in the AREADME file, you are ready to start the installation of the CA Chorus Security Discipline. The SECROLE member that is housed in the <custlib_hlq>.CHRSEC30.CUST.JOBLIB data set contains the variables you specified as part of the unified install process which you will need for the CA Chorus Security Discipline installation process. For more information on installing the Security Discipline, see the CA Chorus *Installation Guide*.

Clean Up the USS Directory (Optional)

Important! This procedure is optional. Do not use this procedure until you complete the entire installation process.

To free file system disk space for subsequent downloads after downloading and processing the pax files for your CA Technologies product, we recommend removing the files from your USS directory. You can delete the following items:

- Pax file
- Product-specific directory that the pax command created and all of the files in it

Follow these steps:

1. Navigate to your Pax ESD USS directory.

   Your view is of the applicable USS directory.

2. Delete the pax file by entering the following command:

   `rm paxfile.pax.Z`

   paxfile.pax.Z

   Specifies the name of the CA Technologies pax file that you downloaded.

   The pax file is deleted.

Note: You can also use TSO ISHELL to navigate to the pax file and paxfile directory and delete them using the D line command.

Chapter 3: Manual Install Process

This chapter manually steps you through the unloading and configuration of the security software prerequisites. The manual method supports CA Datacom/AD and DB2 and lets you install on multiple systems. You can also select specific components of CA Compliance Manager such as Alerts or Logger. To install the CA Chorus for Security and Compliance Management discipline using the manual method, see Addressing General Prerequisites for Manual Installation.

This section contains the following topics:

Pre-Installation Planning Team

The CA Chorus Security and Compliance Discipline installation is a detailed process that requires personnel in several areas of expertise. We suggest that you meet with each of the following team members before the installation begins and review the roles of each person:

- Systems programmer for z/OS
- Storage administrator for DASD allocations
- Security administrator for access permissions and security configuration
- Database administrator for IMS and/or CA Datacom/AD configuration

For this meeting, we recommend that you refer to the platform and discipline *Site Preparation Guide* and *Installation Guide*.

Additionally, given the scope of the installation, we recommend that team members review the entire guide before beginning the installation.

Important! Do not begin the installation until all team members have a clear understanding of their installation responsibilities. Failure to do so can impact your ability to complete the installation in a timely manner.

Migrating CA Chorus for Security and Compliance Management to CA Chorus v4.0

If you are migrating to CA Chorus v4.0, see the following topics that apply to your site. If you are not migrating, skip to the Pre-Installation Planning Decisions for CIA Real-Time Implementation (see page 50).

- Migrate CIA Real-Time Component
- Migrate CA Compliance Manager (see page 49)

Migrate CIA Component

The Compliance Information Analysis (CIA) component has been updated in CA Chorus v4.0 to enable RACF support. Enhancements include the following:

- Addition of the following CIA repository tables to support RACF
  - USERRACF
  - ROLERACF
  - ROLEXRCF
  - PERMRACX
  - RESRACF
  - RACFVARS
  - RESXRACF
- Modifications to the following tables to support RACF:
  - USERACF2
  - USERINFO
  - USERTSS
  - USERTSO
  - USERIDMP
  - ROLEINFO
  - ROLEREC
  - ROLEATTR
  - ROLEEXTR
  - ROLEXREF
  - PERMCOLX
  - PERMFACX
  - PERMLIBX
  - PERMPGMX
  - PERMSYSX
  - RESXREF
  - UDFCHAR
  - SCPRES
  - EIMREC
  - PROXYREC
  - DCOREC

  - ADMNMISC
  - FACCMND
  - FACSITRN
- Updated method for supporting RACF in CIA batch unload and load processes.
- Support added for RACF in a CIA CA Datacom/AD repository.
- The following CIA SAMPJCL jobs were updated to support RACF updates:
  - CIA4BIND
  - CIA4DBLA
  - CIA4DBLD
  - CIA4DB2
  - CIA4DB2D
  - CIA4DCLD
  - CIA4DCMD
  - CIA4DCOM
  - CIA4FUNC
  - CIA4LNKC
  - CIA4LNK1
  - CIA4PLND
  - CIA4SQL1

Follow these steps:

1. Review Implementing CIA Real-Time for CA Chorus for Security and Compliance Management (see page 196) and follow the instructions to perform the following steps for a CA Datacom/AD or DB2 repository implementation:
   - Stop the CIA Real-Time Component
   - Implement the CIA Repository in CA Datacom/AD
     - Start the CA Datacom/AD MUF
     - Link the CIA functions with CA Datacom/AD
     - Delete the CIA repository for CA Datacom/AD
     - Define the CIA repository for CA Datacom/AD
   - Implement the CIA Repository in DB2
     - Start the DB2 subsystem
     - Link the DB2 Modules and Functions
     - Delete the CIA repository for DB2
     - Define the CIA repository for DB2
   - Estimate storage requirements for the Unload data set

     Important! Use the CA ACF2 Worksheet (see page 115) and CA Top Secret Worksheet (see page 117) provided to calculate the amount of space required for the Unload data set.
   - Allocate the Unload data set
   - Unload the security information
   - Load the CIA repository
   - Start the CIA Real-Time component

     Important! If you are using CA ACF2 and updated the ACFFDR, stop and restart the CIA real-time address space to refresh the in-core tables.

Migrate CA Compliance Manager

Important! Do NOT delete or redefine any of your existing CA Compliance Manager repositories, unless you are changing your CA Compliance Manager implementation.

Pre-Installation Decisions for the CIA Real-Time Implementation

Identify the following information to assist with the CIA real-time feature implementation.

Select the CIA Repository

There must be a single CIA repository, containing the account and security policy information from all instances of CA ACF2 and CA Top Secret across an enterprise. This CIA repository can be hosted on any LPAR in the enterprise and can reside in a CA Datacom/AD MUF or in a DB2 subsystem.

Important! We recommend that the CA Datacom/AD MUF or DB2 subsystem be dedicated to the CIA repository. This recommendation helps to ensure that there is no unauthorized access to the security information contained in the repositories.

No integrity issues exist when the CIA repository and the CA Compliance Manager repositories reside on the same LPAR in a single CA Datacom/AD MUF or DB2 subsystem. However, if the CA Compliance Manager Warehouse repository is recording a high volume of security events, hosting the repositories in a single CA Datacom/AD MUF or DB2 subsystem is not recommended.

The CA Chorus server also includes a repository contained in CA Datacom/AD. When the CIA repository is on the same LPAR, **DO NOT** place the CIA repository in the same CA Datacom/AD as the CA Chorus server repository. This set up creates the potential security exposures discussed in the Important note.

When the CA Compliance Manager repositories or CIA repository resides in a CA Datacom/AD MUF, an instance of the CA Datacom Server is required for the CA Datacom/AD MUF. CA Chorus uses the CA Datacom Server to access the information from the repositories.

Follow these steps:

1. If you are using a DB2 repository for CIA, record the DB2 subsystem name in your Site Preparation Worksheet.

   Note: This information is required during the CIA real-time implementation process.

2. If you are using a CA Datacom/AD repository for CIA, record the CA Datacom/AD MUF name in your Site Preparation Worksheet. The default MUF name provided in the CIA sample JCL jobs is CIAMUF, which is recommended.

   Note: This information is required during the CIA real-time implementation process.

Select z/OS Image to Host CIA Repository

Select the z/OS image that hosts the CA Chorus CIA repository. Depending on your site, you can select DB2 or CA Datacom/AD.

The CA Chorus CIA repository reside in a CA Datacom/AD MUF or DB2 subsystem on a single z/OS image. This repository can contain the security information from multiple security databases across your enterprise. This repository is updated from any z/OS image where changes to that security database information can occur. CA Chorus accesses the security information in the CIA repository in servicing CA Chorus functionality.

Select a z/OS image with the following so that the updating and retrieval of the CIA repository information meets your CA Chorus performance criteria:

- licensing to run a CIA subsystem
- performance profile with sufficient resources

Pre-Installation Decisions for the CA Compliance Manager Implementation

Identify the following information to assist with the CA Compliance Manager implementation.

Select the CA Compliance Manager Repositories

CA Compliance Manager can have up to three repositories, depending on which components are running. The repositories are for the Warehouse, Data Mart, and Monitor components. The CA Compliance Manager repositories can reside in a single CA Datacom/AD MUF or a single DB2 subsystem.

Important! We recommend that the CA Datacom/AD MUF or DB2 subsystem be dedicated to the CA Compliance Manager repositories. This recommendation helps to ensure that there is no unauthorized access to the security information contained in the repositories.

No integrity issues exist when the CIA repository and the CA Compliance Manager repositories reside on the same LPAR in a single CA Datacom/AD MUF or DB2 subsystem. However, if the CA Compliance Manager Warehouse repository is recording a high volume of security events, we do not recommend that you host the repositories in a single CA Datacom/AD MUF or DB2 subsystem.

The CA Chorus server also includes a repository contained in CA Datacom/AD. When the CA Compliance Manager repositories are on the same LPAR, **DO NOT** place the CA Compliance Manager repositories in the same CA Datacom/AD as the CA Chorus server repository. This set up creates the potential security exposures discussed in the Important note.

When the CA Compliance Manager repositories or CIA repository resides in a CA Datacom/AD MUF, an instance of the CA Datacom Server is required for the CA Datacom/AD MUF. CA Chorus uses the CA Datacom Server to access the information from the repositories.

Follow these steps:

1. If you are using a DB2 repository for CA Compliance Manager, record the DB2 subsystem name in your Site Preparation Worksheet.

   Note: This information is required during the CA Compliance Manager implementation process.

2. If you are using to use a CA Datacom/AD repository for CA Compliance Manager, record the CA Datacom/AD MUF name in your Site Preparation Worksheet. The default MUF name provided in the CA Compliance Manager sample JCL jobs is CMGRMUF, which is recommended.

   Note: This information is required during the CIA CA Compliance Manager implementation process.

Select z/OS Image to Host CA Compliance Manager Repositories

Select the z/OS image that hosts the CA Chorus CA Compliance Manager repositories. Depending on your site, you can select DB2 or CA Datacom/AD.

The CA Chorus CA Compliance Manager repositories reside in a CA Datacom/AD MUF or DB2 subsystem on a single z/OS image. These repositories can contain the security information from multiple security databases across your enterprise. These repositories are updated from any z/OS image where changes to that security database information can occur. CA Chorus accesses the security information in the CA Compliance Manager repositories in servicing CA Chorus functionality.

Select a z/OS image with the following so that the updating and retrieval of the CA Compliance Manager repository information meets your CA Chorus performance criteria:

- licensing to run a CA Compliance Manager subsystem
- performance profile with sufficient resources

Site Preparation Worksheet

As part of pre-installation planning for the CA Chorus for Security and Compliance Management, review and complete the Site Preparation Worksheet (see page 179). The worksheet contains all of the information and customizable values required to complete the pre-installation and installation process for this discipline.

Software Requirements

The following software is required for the CA Chorus Security and Compliance Discipline. To verify that the software with the latest maintenance has been installed contact your installer.

Note: For more information about installing and configuring these products, see the product installation and implementation documentation.

- CA ACF2 r15 or CA Top Secret r15 with all current CA Chorus FIXCAT maintenance for these products. The FIXCAT label is CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.*, where * indicates the version of CA Chorus that you are installing.
- For information about current product maintenance, see http://ca.com/support. Select z/OS compatibilities located under the Security, Control and Audit section.

  Note:

  - As part of pre-installation planning, you determined if you are implementing Compliance Information Analysis (CIA) for CA Chorus and if so, if you are using a CA Datacom/AD or DB2 CIA repository.
  - The CA Chorus LMP key must be available on every z/OS image where the CIA real-time feature is enabled.

- IBM RACF Version 1 Release 13 with current maintenance. For information about current RACF product maintenance, contact IBM.

  Note: The CA Chorus LMP key must be available on every z/OS image where IBM RACF is installed. When the IBM RACF unload utility is executed, CA Chorus performs an LMP check. Without the key, the RACF unload utility cannot be used.

- CA Compliance Manager Version 2.0 with all current CA Chorus FIXCAT maintenance for these products. The FIXCAT label is CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.*, where * indicates the version of CA Chorus that you are installing.

  Note the following:

  - Follow the steps in this guide to configure and implement CA Compliance Manager components for CA Chorus.
  - As part of pre-installation planning, you determined which CA Compliance Manager components and repositories you are using.
  - CA Chorus Security and Compliance Discipline requires the configuration of CA Datacom/AD or DB2 repositories, if you are using the Warehouse, Monitor, and Data Mart components.
  - CA Chorus Security and Compliance Discipline requires the Router. The Router ensures all qualifying external security manager (ESM) events are passed to one or more active components. The Alerts, Logger, Monitor, and Warehouse components are optional based on the processing you want done. For example:
    - Send CA Chorus alerts to the Alerts module using the Alerts or Monitor components.
    - Load events into the CA Compliance Manager repository from the Logger component logstream using the Data Mart utility.
    - Write events directly to the CA Compliance Manager repository using the Warehouse component.

- CA Datacom/AD r14
  - CA Chorus does not support CA Datacom/DB. If you have CA Datacom/DB installed, install CA Datacom/AD and reference these libraries when installing CA Chorus.

    Important! If you are using IBM DB2 to manage the CIA and CA Compliance Manager security repositories, this software is not required for CA Chorus for Security and Compliance Management.
  - For CA Chorus for Security and Compliance Management sites using CA Datacom/AD for Compliance Information Analysis (CIA) or CA Compliance Manager data:
    - CA Datacom Server includes a JDBC/ODBC component that runs under UNIX System Services (USS). These components are required for this discipline. To install these required components, including the CA Datacom Server, from the CA CSM install wizard, select Base Install + USS Client for DBSRV, FMID CAYTE02
    - A CA Datacom/AD MUF and Server are required per LPAR. Due to the nature of the data stored, we recommend a unique MUF which can be used for CIA and CA Compliance Manager data. Do not reuse an existing CA Datacom/AD MUF and server. This Guide documents the required steps to create and start CA Datacom/AD MUFs for CIA and CA Compliance Manager.
- CA LDAP Server r15.1 with all current CA Chorus FIXCAT maintenance for these products. The FIXCAT label is CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.*, where * indicates the version of CA Chorus that you are installing.

  Note: The ability to modify and delete users in the CA Chorus Investigator is based on new functionality in CA LDAP Server r15.1.
- CA DSI Server r15.1 with all current CA Chorus FIXCAT maintenance for these products. The FIXCAT label is CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.*, where * indicates the version of CA Chorus that you are installing.

  Note: The CA LDAP Server installation files include CA DSI Server.

- IBM Software—Verify with your site's database administration that the following IBM software is available on the systems where CA Chorus Security and Compliance Discipline is installed.
  - IBM DB2 V8 New Function Mode (NFM), DB2 9, or DB2 10

    Important! If you are using CA Datacom/AD r14 to administer the CIA and CA Compliance Manager repositories, this software and the following services are not required.

    - IBM Resource Recovery Services (RRS) for z/OS to manage the Resource Recovery Services Attachment Facility (RRSAF)

      Note: RRSAF is the DB2 attachment facility that this discipline uses. For more information about implementing RRS for your DB2 systems, see the IBM Resource Recovery Services documentation.

    - Distributed Data Facility (DDF)
    - Workload Manager (WLM)
  - Open Database Connectivity (ODBC)
  - JDBC Universal Driver

    Note: Install the IBM Data Server Driver for JDBC and SQLJ so that the needed stored procedures are installed.
- PC software that is required for each user:
- Adobe Flash Player 9.0.124 or above

At the release of Version 4.0, we certified CA Chorus for Microsoft Windows Internet Explorer 9 and 11, and Mozilla Firefox 23 through 32. As new browsers are released, we will certify them and update CA Chorus Browser Compatibility. You can use CA Chorus in new browser releases; however, until each release officially passes our certification test, you may face intermittent issues. If you encounter issues, contact support, and we will resolve your issue.

Note the following:

- Disable pop-up blockers for your browser before you access your CA Chorus instance.
- 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.

Server Requirements

Confirm that your site meets the following requirements:

Real storage

100 MB heap memory for CA Chorus for Security and Compliance Management plus 2450 MB heap memory for CA Chorus

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 meets the following system requirements:

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.

Disk

Approximately 200 cylinders are required for CA Chorus for Security and Compliance Management installation.

Approximately 160 cylinders are needed on the zFS that holds the CA Chorus for Security and Compliance Management pax installation file.

Note: This space can be reclaimed after installation.

Additional storage requirements exist for real-time Compliance Information Analysis (CIA) and CA Compliance Manager administration.

Important! To help improve system performance, we recommend that you do not load the CIA and CA Compliance Manager databases and log stream all on one pack.

Note: For more information about additional storage requirements, see the CA ACF2, CA Top Secret, and CA Compliance Manager product documentation.

Target Libraries

The following table shows the data set space requirements by tracks for the CA Chorus for Security and Compliance Management target libraries:

Data Set Name	Tracks
CE1MXML	250
CE1MJCL	50
CE1MOPTV	10
CE1MZFS	1100 (zFS directory)

Distribution Libraries

The following table shows the data set space requirements for the CA Chorus for Security and Compliance Management distribution libraries:

Data Set Name	Tracks
AE1MJCL	250
AE1MXML	50
AE1MOPTV	10
AE1MZFS	1100 (zFS directory)

Port Requirements

To configure CA LDAP Server and CA DSI Server to work with CA Chorus for Security and Compliance Management discipline, identify the CA LDAP Server and CA DSI Server that you plan to use with this discipline. The port that each server is listening on and the suffix values defined for each backend defined to the CA LDAP Server is required. These jobs are run during installation of CA Chorus and disciplines. For more information, see the CA Chorus Installation Guide.

Confirm that the ports you intend to use are available.

This discipline uses the following listening ports:

CA LDAP Server port

Listens for CA LDAP Server requests. This server is required for policy administration. Specify one port per CA LDAP Server. You define this port in the slapd.conf configuration file.

CA DSI Server port

Specifies the port number that accepts CA DSI Server requests. This server is required for CIA real-time updates, simulation, and the Security Command Manager module. When administering security on remote LPARs, a CA DSI Server port is required on each remote LPAR.

For each CA DSI Server running remotely, assign a port number to accept incoming server requests. You define this port in the dsi.conf configuration file that is associated with each CA DSI Server.

Security Requirements

The following procedure is required for the CA Chorus for Security and Compliance Management discipline to obtain the JCL jobs that define required security authorizations.

Follow these steps:

1. Unpack the CA Chorus for Security and Compliance Management pax file by entering the following commands under UNIX System Services (USS):

   ```
   cd <chorussec_install_directory>
   ```

   ```
   pax E1M40G0.pax.Z
   ```

2. Extract the following jobs from the pax file into *your_chorussec_hlq.*CE1MJCL:

   CA ACF2 - E1MIA021

   CA Top Secret - E1MIT021

3. Choose the appropriate job for your external security manager (ESM).

   Edit and submit this job during the site preparation process. See Addressing Security Requirements (see page 191).

CA Datacom/AD and Program Control

You need program control on the shared objects that are specifically loaded in CA Chorus Application Server. Add the program control attribute to ensure that the program is trusted for server activities.

Important! Complete this procedure after you apply any CA Datacom/AD server for USS maintenance.

Follow these steps:

1. Change the directory to DBSRV_HOME/lib:

   ```
   cd <DBSRV_HOME> /lib
   ```

2. Add program control:

   ```
   extattr +p CADCDB64 CADCJDBC libcadcdb64.so cadcjdbc.jar
   ```

3. List all modules showing their extended attributes:

   ```
   ls -lE
   ```

4. Ensure that the p (that is, program controlled) attribute appears on the applicable files.

Example

```
# cd /<site-specific path>/datacom/lib
# ls -lE CADCDB64 CADCJDBC libcadcdb64.so cadcjdbc.jar
-rwxrwxrwx  -ps-  2 userID  OMVSDFG   380928 May  1 14:24 CADCDB64
-rwxrwxrwx  -ps-  2 userID  OMVSDFG   311990 May  1 14:24 CADCJDBC
-rwxrwxrwx  -ps-  2 userID  OMVSDFG   311990 May  1 14:24 cadcjdbc.jar
-rwxrwxrwx  -ps-  2 userID  OMVSDFG   380928 May  1 14:24 libcadcdb64.so
```

Chapter 4: Addressing Security Requirements

Define Security Authorizations for CA Chorus for Security and Compliance Management

The E1MIA021 for CA ACF2 and E1MIT021 for CA Top Secret job configures security authorizations for the CA Chorus for Security and Compliance Management discipline. The following authorizations are included in these jobs:

- Defines CA Chorus installer user id privileges for:
  - UNIX System Services (USS)
  - z/OS
- Authorizes CA Chorus users to access USS resources
- Authorizes users to work in CA Chorus
- Configures PassTickets for user authentication

Follow these steps:

1. Edit the E1MIA021 for CA ACF2 and E1MIT021 for CA Top Secret job in the following library:
   - *your_chorussec_hlq*.CE1MJCL

   Modify the job to conform to your installation standards. Follow the instructions in the notes and the customization sections of the job to customize the job for your environment.
2. Submit the job.

   The job runs and completes.
3. Review the output of the job to verify that the security definitions are successfully defined.

Define the Started Task User ID for CA LDAP Server

The CDT9ACID and CDT9LID jobs create the following security authorizations for CA LDAP Server:

- Permissions to data sets (such as TCP/IP)
- Facility accesses for BPX server and daemon

Important! This should have been completed as part of the CA LDAP Server install. If not, use this procedure to configure CA LDAP Server in accordance with your site specifications. Complete these post-configuration steps before you start the CA LDAP Server Server:

Follow these steps:

1. Edit the job to define STC user IDs. Change the HOME in the job to the directory name where you installed LDAP.
   - CA ACF2 - CDT9LID in *your_ldap_hlq*.CDT9JCL
   - CA Top Secret - CDT9ACID in *your_ldap_hlq*.CDT9JCL
2. Submit the job.
3. Verify the job output.

   The STC user IDs are defined for the installation.
4. Edit the LDAPR15 STC PROC in *your_ldap_hlq*.CDT9JCL as follows:
   a. Change all occurrences of *INSTALL_DIR* to the path name of the directory that contains the HFS files.
   b. (If CA Compliance Manager is installed) Change the HLQ argument on the second line to the high-level qualifier of the policy file. Change the VOL argument on the fourth line so that it includes the policy file's VOLSER.
   c. Uncomment the lines that define the policy and journal files at the end of the proc.

   The LDAPR15 STC PROC is updated.
5. Copy the LDAPR15 STC PROC from *your_ldap_hlq*.CDT9JCL into your proclib.
6. Update the slapd.env file to add the correct directoryname (PATH and LIBPATH)

   The slapd.env file is updated.
7. Update the slapd.conf file

   Important! For more information on updating these files, see the CA LDAP Server *Product Guide* and *Installation Guide*.
8. Start the STC using the LDAPR15 job.

Define the Started Task User ID for CA DSI Server

The DSILID and DSIACID jobs create the started task user id and assign appropriate security authorizations for CA DSI Server installation.

Important! This should have been completed as part of the CA LDAP Server install. If not, use this procedure to configure CA DSI Server in accordance with your site specifications.

Follow these steps:

1. Edit the job to define STC user IDs. Change the HOME in the job to the directory name where you installed LDAP.
   - CA ACF2 - DSILID in *your.ldap.hlq.*CDT9JCL
   - CA Top Secret - DSIACID in *your_ldap_hlq.*CDT9JCL
2. Submit the job.
3. Verify the job output.

   The STC user IDs are defined for the installation.
4. Update the dsi.env file to add the correct directory name (PATH and LIBPATH).

   The dsi.env file is updated.
5. Update the dsi.conf file to address the following areas:
   a. Review the documentation in the file for each of the preset values and change any that you need to. You must change the host option. Comment out the line or supply a valid domain name. If you provide a domain name, the domain name must be associated with one of the interfaces of the system on which the DSI server is to run. In this case, the DSI server accepts connections only if they arrive over the designated interface. Commenting out the line allows the DSI server to accept connections that arrive over all interfaces.
   b. Review the port setting. The default in the file is 1490. If this port is not acceptable, change it to a setting that meets your site-specific requirements.

   The dsi.conf file is updated.
6. Edit the DSIR15 STC PROC in SAMPJCL to change all occurrences of *INSTALL_DIR* to the path name of the directory that contains the HFS files.

   The DSIR15 STC PROC is updated.
7. Copy the DSIR15 STC PROC from SAMPJCL into your proclib.

   The DSIR15 STC PROC is in your proclib.
8. Start the STC using the DSIR15 job.

Define Security Authorizations for CA DSI Server

The DSICIA job defines the security authorizations for CA DSI Server to enable the server to access the CIA repository. It assigns the CA DSI Server authorization to access the CA Datacom/AD or DB2 database plan. When CIA real-time processing is implemented, a CIA plugin module in the CA DSI Server performs processing against the CIA repository.

Important! This should have been completed as part of the CA DSI Server install. If not, use this procedure to configure CA DSI Server in accordance with your site specifications.

Follow these steps:

1. Edit the DSICIA job in *your_ldap_hlq*.CDT9JCL.

   Modify the job to conform to your installation standards. Follow the instructions in the notes and the customization sections of the job to customize the job for your environment.

2. Submit the job.

3. Verify the job output.

   The CA DSI Server security authorizations are defined for the installation.

Important! Verify that you have assigned the CA DSI Server authorization to access the CA Datacom/AD or DB2 database plan.

Configure PassTickets to Connect to CA Datacom/AD or DB2

Important! If you are installing CA Chorus for Security and Compliance Management, PassTickets are needed for the CA Chorus server to connect to the following functions. If you are using CA ACF2 or CA Top Secret, PassTicket configuration was already completed in the E1MIA021 for CA ACF2 or the E1MIT021 for CA Top Secret job. If you are using IBM RACF, see Use IBM RACF to Configure PassTickets for Database Connections and Use IBM RACF to Configure PassTickets to Connect to CA LDAP Server.

- CA Datacom/AD or DB2 at startup
- CA LDAP Server

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

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

The CA Chorus web service calls the z/OS security product to generate a PassTicket for access authorization.

The PassTicket is sent with the user request to the component, possibly on a different z/OS system.

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

Configuration information for local and remote systems is provided in PassTicket Configuration for CA Chorus Systems.

PassTicket Configuration for CA Chorus Systems

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 specific 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) 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 are required by the CA Chorus disciplines. This type of system is known as a CA Chorus remote system.

The CA Chorus server system provides the point of entry for all 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.

PassTicket configuration for the z/OS security product must be done on each z/OS system that is hosting a component that is used by CA Chorus. Configure PassTickets in your z/OS security products to enable the generation and validation of connections that are required for CA Chorus disciplines. Note the following:

- If the CA Chorus server system and the remote systems share a security database, no additional 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.

PassTicket Configuration to Connect to CA Datacom/AD

The CA Chorus server uses a PassTicket to log in to CA Datacom/AD and read security information from the CIA and CA Compliance Manager databases.

Important! If you are using CA ACF2 or CA Top Secret, PassTicket configuration was completed in the E1MIA021 (for CA ACF2) and E1MIT021 (for CA Top Secret) job. If you are using IBM RACF, see Use IBM RACF to Configure PassTickets for Database Connections (see page 68) and Use IBM RACF to Configure PassTickets to Connect to CA LDAP Server (see page 71). Create multiple PassTickets if your CIA and CA Compliance Manager databases are in different locations. One is required for each database.

If you are using CA Datacom/AD for CIA or CA Compliance Manager, configuration is also required for the CA Datacom/AD Server to enable PassTicket authentication. The CA Datacom/AD Server provides a gateway from the JDBC and ODBC drivers to the CA Datacom/AD MUF.

Implementation and configuration of CA Datacom/AD Server for CIA is performed later in this guide. See Implement CA Datacom/AD Server for CIA.

Implementation and configuration of CA Datacom/AD Server for CA Compliance Manager is performed later in this guide. See Implement CA Datacom/AD Server for CA Compliance Manager.

Use IBM RACF to Configure PassTickets for Database Connections

This example shows how to use IBM RACF to configure PassTickets for connecting to DB2 or CA Datacom/AD to read information from the CIA and CA Compliance Manager databases. An experienced security administrator must perform this procedure.

Note: Before you begin this procedure, verify that the PTKTDATA class and ownership for the PassTicket resource (IRRPTAUTH) have not been defined.

Follow these steps:

1. Activate the PassTicket class by entering the following command:

   ```
   SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
   SETROPTS GENERIC(PTKTDATA)
   ```

2. Define profiles for the application in the PTKTDATA class for the application and specify the session keys:

   ```
   RDEFINE PTKTDATA applid SSIGNON(KEYMASKED(FEDCBA9876543210))
   APPLDATA('NO REPLAY PROTECTION')
   ```

   applid

   Defines the application ID used for PassTicket validation to authenticate connections to the server.

   - For DB2, use the DB2 command -DISPLAY DDF to determine the appropriate value to use for the PassTicket application name.

     If GENERICLU is not defined, replace *applid* with the second part of the LUNAME.

     If GENERICLU is defined, use the second part of GENERICLU.

     If neither LUNAME or GENERICLU are defined, use the value of the IPNAME.

     Sample output from the -DISPLAY DDF command follows:

     LOCATION LUNAME GENERICLU

     DA0GPTIB example.*text1* example.*text2*

     TCPPORT=5122 SECPORT=5193 RESPORT=5124 IPNAME=-NONE

     In the sample output, *text1* and *text2* represent the LUNAME and GENERICLU name, respectively.

     Note: When issuing a DB2 command from the z/OS console, replace the hyphen (-) with the specific command prefix for the DB2 region.

   - For CA Datacom/AD, specify the MUF name.

   KEYMASKED

   Defines an encryption key for the application using values that are different from the values in the sample syntax.

   Note: The sample syntax demonstrates a complete key value of 16 hexadecimal digits (creating an 8-byte or 64-bit key). Each application key must be the same on all systems in the configuration and the values must be kept "secret."

   APPLDATA('NO REPLAY PROTECTION')

   Use the same PassTicket multiple times.

The CA Chorus session keys are defined.

Note: This example demonstrates a complete key SESSKEY value of 16 hexadecimal digits (creating an 8-byte or 64-bit key). Keys consist of 16 random hexadecimal digits. Each application key must be the same on all systems in the configuration and the values must be kept "secret." Select different values from the ones shown in the examples.

3. Define profiles for PassTicket generation:

   a. Permit access to the applid PassTicket session key value for each user that is permitted to access the application.

   ```
   RDEFINE PTKTDATA IRRPTAUTH.applid.* UACC(NONE)
   PERMIT IRRPTAUTH.applid.* ID(stc-userid) ACCESS(UPDATE)
   CLASS(PTKTDATA)
   ```

   stc-userid

   Specifies the started task user ID created in ETJI095R in *your_chorus_hlq*.CETJJCL. This ID must be able to generate PassTickets for any user. The default is CHORADM.

   b. Alternatively, you can create a group. For example:

   ```
   ADDGROUP ETJDB2GR
   CONNECT CHORUSR1 GROUP(ETJDB2GR)
   CONNECT CHORUSR2 GROUP(ETJDB2GR)
   ...
   CONNECT CHORUSRN GROUP(ETJDB2GR)
   RDEFINE PTKTDATA IRRPTAUTH.applid.ETJDB2GR
   OWNER(installer-userid) UACC(NONE)
   PERMIT  IRRPTAUTH.applid.ETJDB2GR ID(stc-user) AC(UPDATE)
   CLASS(PTKTDATA)
   ```

   In this example, ETJDB2GR defines the group for the CA Chorus Security and Compliance Discipline users; CHORUSRx defines the specific users to the group; the RDEFINE command defines the resource to enable PassTicket generation for the group members; the PERMIT command enables the CA Chorus Application Server user to generate PassTickets to the application for group members.

4. Refresh the PTKTDATA class:

   ```
   SETROPTS RACLIST(PTKTDATA) REFRESH
   ```

CA Chorus for Security and Compliance Management PassTicket Configuration to Connect to CA LDAP Server

Important! If you are using CA ACF2 or CA Top Secret, PassTicket configuration was already completed in the E1MIA021 for CA ACF2 or the E1MIT021 for CA Top Secret job. If you are using IBM RACF, see Use IBM RACF to Configure PassTickets to Connect to CA LDAP Server.

CA Chorus for Security and Compliance Management uses PassTicket security to connect to CA LDAP Server to launch components from the Quick Links module without requiring an additional user login. All systems using Passtickets must have identical application names and session keys for all nodes on the network. For CA Chorus for Security and Compliance Management, the default application ID is CALDAP.

Note: An experienced security administrator familiar with PassTicket configuration must execute this process. For information about using IBM RACF, see the IBM documentation.

Use IBM RACF to Configure PassTickets to Connect to CA LDAP Server

This example shows how to use IBM RACF to configure PassTickets to connect to CA LDAP Server from the Quick Links module in CA Chorus. An experienced security administrator must perform this procedure.

Note: Before you begin this procedure, verify that the PTKTDATA class and ownership for the PassTicket resource (IRRPTAUTH) have not been defined.

Follow these steps:

1. Activate the PassTicket class by entering the following command:

```
SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
SETROPTS GENERIC(PTKTDATA)
```

2. Define profiles for the application in the PTKTDATA class for the application and specify the session keys:

   ```
   RDEFINE PTKTDATA applid SSIGNON(KEYMASKED(FEDCBA9876543210))
   APPLDATA('NO REPLAY PROTECTION')
   ```

   applid

   Defines the application ID used for PassTicket validation to authenticate connections to the server. Replace *applid* with CALDAP.

   KEYMASKED

   Defines an encryption key for the application using values that are different from the values in the sample syntax.

   Note: The sample syntax demonstrates a complete key value of 16 hexadecimal digits (creating an 8-byte or 64-bit key). Each application key must be the same on all systems in the configuration and the values must be kept "secret."

   APPLDATA('NO REPLAY PROTECTION')

   Lets you use the same PassTicket multiple times.

   The CA Chorus session keys are defined.

   Note: This example demonstrates a session key value of 16 hexadecimal digits (creating an 8-byte or 64-bit key). Use a different value when you define your session keys. Each application key must be the same on all systems in the configuration and the values must be kept "secret."

3. Define profiles for PassTicket generation:

   a. Permit access to the applid PassTicket session key value for each user that is permitted to access the application.

      ```
      RDEFINE PTKTDATA IRRPTAUTH.applid.* UACC(NONE)
      PERMIT IRRPTAUTH.applid.* ID(stc-userid) ACCESS(UPDATE)
      CLASS(PTKTDATA)
      ```

      stc-userid

      Refers to the user ID created in Create a CA Chorus User ID. CHORADM by default. This user ID must be able to generate PassTickets for any user.

   b. Alternatively, you can create a group. For example:

      ```
      ADDGROUP ETJDB2GR
      CONNECT CHORUSR1 GROUP(ETJDB2GR)
      CONNECT CHORUSR2 GROUP(ETJDB2GR)
      ...
      CONNECT CHORUSRN GROUP(ETJDB2GR)

      RDEFINE PTKTDATA IRRPTAUTH.applid.ETJDB2GR
      OWNER(installer-userid) UACC(NONE)
      PERMIT  IRRPTAUTH.applid.ETJDB2GR ID(stc-user) AC(UPDATE)
      CLASS(PTKTDATA)
      ```

      In this example, ETJDB2GR defines the group for the CA Chorus Security and Compliance Discipline users; CHORUSRx defines the specific users to the group; the RDEFINE command defines the resource to enable PassTicket generation for the group members; the PERMIT command enables the CA Chorus Application Server user to generate PassTickets to the application for group members.

4. Refresh the PTKTDATA class:

   ```
   SETROPTS RACLIST(PTKTDATA) REFRESH
   ```

Configure CA LDAP Server Resource Authorizations for CA Compliance Manager Policies and Reports

When a user tries to access information through the Compliance Policy Administration interface, a resource authorization check occurs against the logged in user ID. The RACROUTE AUTH call submitted from the interface uses one of two entities. Additionally, the interface uses one of two possible access levels depending on the type of data the user is trying to access.

Because all CA Compliance Manager interface requests are processed through the CA LDAP Server, the following parts of the resource authorization check parameters are configurable:

- The high-level qualifier that is used when the entity is constructed
- The resource class

Follow these steps:

1. Customize control access by modifying the values in the CA LDAP Server slapd.conf file using the following parameters:

   Important!: Skip this step if you accept the default values for these parameters.

   CMGRPolicyEntity

   Indicates the high-level qualifier to use when constructing the entity name.

   Default: CMGR

   CMGRPolicyClass

   Indicates the resource class that RACROUTE AUTH call uses.

   Default: CACMGR

   The full entity name is a concatenated value consisting of the high-level qualifier value specified in the CMGRPolicyEntity parameter and REPORTS or POLICY. The latter depends on the area of the CA Compliance Manager interface the user is accessing. The following table includes examples:

Pane Task	Entity	Access Level
Reports	CMGR.REPORTS	READ
Create a policy set	CMGR.POLICY	UPDATE
Modify a policy set	CMGR.POLICY	UPDATE
Delete a policy set	CMGR.POLICY	UPDATE
Create a policy statement	CMGR.POLICY	UPDATE

Pane Task	Entity	Access Level
Modify a policy statement	CMGR.POLICY	UPDATE
Delete a policy statement	CMGR.POLICY	UPDATE

For detailed control access and option information, see the *CA LDAP Server for z/OS Product Guide*.

2. Modify the following CA Compliance Manager jobs in CAI.CEIQJCL0 to match the CMGRPolicyEntity and CMGRPolicyClass values in defining these resource authorizations for CA Compliance Manager:

   - CA ACF2 - CMGRIACF
   - CA Top Secret - CMGRITSS
   - IBM RACF CMGRIRAC

   Important! Skip this step if you accept the default values for the CMGRPolicyEntity and CMGRPolicyClass parameters in the previous step.

   The high-level qualifier value that is used for the entity is the value specified in the slapd.conf file CMGRPolicyEntity parameter.

Define RRSAF Authorizations for CA Chorus for Security and Compliance Management

CA Chorus Security and Compliance Discipline requires a resource permission for the Resource Recovery Services Attachment Facility (RRSAF). RRSAF functions as the connection authorization mechanism for users connecting to DB2 systems. When an RRSAF connection is attempted, DB2 verifies whether the caller is authorized to use RRSAF. The security administrator must create a resource permission for each started task that is associated with the CA LDAP Server, CA DSI Server, CIA Real-Time, and CA Compliance Manager components.

The RRSAF resource checks are performed on every system that CA Compliance Manager writes to DB2. Perform these resource checks on every system that the warehouse or monitor components are running on.

Note: For more information about managing access to the RRSAF security environment, see the *IBM DB2 Administration Guide.* For more information about the IDENTIFY function for RRSAF, see the *IBM Application Programming and SQL Guide*.

RRSAF authorizations for CA DSI Server are defined in the following job:

- CIADSI - CA DSI Server

This job was run during the Define the Security Authorizations for CA DSI Server procedure in this guide.

RRSAF authorizations for CIA Real-Time component are defined in the following jobs:

- CIARTACF - CA ACF2
- CIARTTSS - CA Top Secret

These jobs are run during the Define the Security Authorizations for CIA Real-Time Component process.

RRSAF authorizations for CA Compliance Manager are defined in the following jobs.

- CMGRIACF - CA ACF2
- CMGRITSS - CA Top Secret
- CMGRIRAC - RACF

These jobs are run during the Define the Security Authorizations for CA Compliance Manager process.

Define Security Authorizations for CIA Real-Time Component (CA ACF2)

If you are using CA ACF2, create the CA ACF2 security environment required for the CIA real-time component.

The CIARTACF job does the following:

- Defines an STC logonid for the CIA real-time component address space with the unscoped AUDIT privilege and defines the OMVS and group profiles required for USS capabilities.
- Gives the STC logonid access to the CIA real-time component data sets.
- Defines the CIA real-time GSO CHORUS record.

  When specified, the following fields in the CA ACF2 GSO CHORUS record enable the recording of update requests to the CIA logstream.

  - CIA
  - CIALOG
  - CIASTG(25|nn)
  - CIAHOST*(CIA DSI host name*)
  - CIAPORT(*nn*)

The CA ACF2 Global System Option (GSO) CHORUS record provides the information required by the CIA real-time component to connect to the DSI server and to read and process the update requests from the CIA logstream.

CIA|NOCIA

Specifies whether CIA real-time updates are active or inactive. When CIA is specified at CA ACF2 startup, it will be started automatically. The default is NOCIA.

CIASTART|NOCIASTART

Specifies whether the CIA real-time component started task is automatically started during CA ACF2 initialization.

CIALOG

Specifies the name of the log stream used by the CIA real-time process. This name must match the logstream name in the CIALOGST job that created the logstream.

CIAPROC(*CIARTUPD|CIA started procedure name*)

Specifies the procedure name for the CIA real-time component started task procedure.

CIASYSID(*CIA sysid used in the CIA database*)

Specifies the SYSID parameter value that was used for this security image when its information was loaded into the CIA repository.

This option allows multiple z/OS images to update a single security image in CIA. When a security product database is shared across multiple z/OS images, each of those images must use the CIASYSID control option to specify the SYSID of the single image that was unloaded.

CIASTG(25|nn)

Specifies the maximum amount of above the bar (64 bit) storage in the ACF2 address space that is used to temporarily hold the queue of update requests that are waiting to be written out to the CIA logstream.

CIAHOST*(CIA DSI host name*)

Specifies the 1-to-255 character host name for the CA DSI Server on the z/OS image that hosts the CIA repository. For more information, see the CA DSI Server *Installation Guide*.

CIAPORT(*nn*)

Specifies the port number for the CA DSI Server on the z/OS image that hosts the CIA repository. For more information, see the CA DSI Server *Installation Guide*.

Follow these steps:

1. Edit the CIARTACF job in CAI.CAX1JCL0.

   Important! DO NOT activate CIA real-time recording in this job. Activation is done later in this guide.

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and the Customization sections of the job to customize the job for your environment.

2. Submit the CIARTACF job.

   The job runs and completes.

3. Verify the output of the CIARTACF job.

   The CIA real-time component is authorized to access security data and send real-time updates.

Define Security Authorizations for CIA Real-Time Component (CA Top Secret)

If you are using CA Top Secret, create the CA Top Secret security environment required for the CIA real-time component. Modify and run the CIARTTSS sample job.

The CIARTTSS job does the following:

- Creates the STC ACID with unscoped control authority (type SCA)
- Gives the ACID administrative authorities and permissions required to run CIA real time
- Defines the OMVS and group profiles required for USS capabilities
- Assigns the STC ACID to the CIA real-time task in the STC

Follow these steps:

1. Edit the CIARTTSS job in CAI.CAK0JCL0.

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and the Customization sections of the job to customize the job for your environment.

2. Submit the CIARTTSS job.

   The job runs and completes.

3. Verify the output of the CIARTTSS job.

   The CIA real-time component is authorized to access security data and send real-time updates.

Define Security Authorizations for CIA Real-Time CA Datacom/AD MUF

If you are using CA Datacom/AD for the CIA repository, before starting the CA Datacom/AD MUF, you must create the definitions for the MUF and the CIA repository as well as the authorizations for the users who access the CIA repository.

Follow these steps:

1. Edit the CIASECC job in one of the following libraries:
   - CA ACF2 - CAI.CAX1JCL0.
   - CA Top Secret - CAI.CAK0JCL0

   Modify the job to conform to your installation standards. Follow the instructions in the job to customize the job for your environment.
2. Submit the CIASECC job.
3. Review the output of the CIASECC job to verify that the security definitions are successfully defined.

Define Security Authorizations to Run the TSSFAR Utility (CA Top Secret)

The following users must be authorized to run TSSFAR:

- A MSCA
- A user with USE access to entity TSSUTILITY.TSSFAR in the CASECAUT resource class

Access may be granted by an administrator by issuing the following command:

```
TSS PERMIT(user) CASECAUT(TSSUTILITY.TSSFAR) ACCESS(USE)
```

Define Security Authorizations to Run the CIA Unload Utility

You must authorize users to run the CIA Unload utility.

Follow these steps:

1. If you are using CA ACF2, allow only users who have an unscoped SECURITY attribute in their logonid to run the CIA Unload utility.
2. If you are using CA Top Secret, allow only users who have an unscoped SECURITY attribute in their ACID to run the CIA Unload utility.

Define Security Authorizations for CA Compliance Manager

In the pre-installation planning phase, you determined which CA Compliance Manager components and repositories to implement. This affects how you customize the security definitions required for CA Compliance Manager in the jobs provided.

The security definition jobs for CA ACF2, CA Top Secret, and IBM RACF (CMGRIACF, CMGRITSS, and CMGRIRAC) define the security environment for all of the CA Compliance Manager components by creating the security definitions for the MUF and the CA Compliance Manager repositories and the authorizations for the users who access the repositories.

These jobs do the following:

- Define the CA Compliance Manager started task user (STC) IDs and gives the STC users USS capabilities for the following:
  - Define the z/OS USS Groups to the ESM
  - Assign a z/OS USS Group to the STC users in the ESM
  - Assign a z/OS USS UID to the STC users in the ESM
  - Assign the STC users to a default group in the ESM

  Note: The name of the STC user created is the same as the procedure name of the started task (e.g., CMGRRTR, CMGRMON, CMGRALRT, CMGRWHSE, CMGRLOGR,).
- Permit access to datasets
- Permit access to datasets for DB2
- Permit access to resources
- Permit access to resources for DB2
- Permit access to DB2 resources
- Define security for CA Datacom/AD MUF and repositories

Follow these steps:

1. Edit the appropriate job in CAI.CEIQJCL0 for your security product:

   CMGRIACF for CA ACF2

   CMGRITSS for CA Top Secret

   CMGRIRAC for IBM RACF

   Modify the job to conform to your installation standards. Follow the instructions in the job to customize the job for your environment.
2. Submit the job.
3. Review the output of the job to verify that the security definitions are successfully defined.

4. Verify that the Warehouse component is authorized to access the Warehouse repository by checking the job output in the following cases:

   - If you are implementing a CA Datacom/AD Warehouse repository, verify that you created appropriate authorizations. See the job output of the CMGRIACF, CMGRITSS, and CMGRIRAC jobs respectively, if you are running CA ACF2, CA Top Secret, or IBM RACF.
   - If you are implementing a DB2 Warehouse repository and use native DB2 security, verify the appropriate authorizations are created during execution of the CMGRIDB2 installation job, which defines the DB2 Warehouse repository. See the job output of the CMGRIDB2 installation job.
   - If you are using CA ACF2 Option for DB2 or CA Top Secret Option for DB2 for your DB2 security, the appropriate authorizations were created during the execution of the CMGRIACF or CMGRITSS jobs, respectively. See the job output of the CMGRIACF or CMGRITSS jobs.

     Note: This action helps ensure that records can be successfully inserted into the Warehouse repository.

5. Verify that the Monitor component is authorized to access the Monitor repository by checking the job output in the following cases:

   - If you are implementing a CA Datacom/AD Monitor repository, verify that you created appropriate authorizations. See the job output of the CMGRIACF, CMGRITSS, and CMGRIRAC jobs respectively, if you are running CA ACF2, CA Top Secret, or IBM RACF.
   - If you use native DB2 security, the appropriate authorizations are created during execution of the CMGRIDB2 installation job, which defines the DB2 Warehouse repository. See the job output of the CMGRIDB2 installation job.
   - If you are using CA ACF2 Option for DB2 or CA Top Secret Option for DB2 for your DB2 security, the appropriate authorizations were created during the execution of the ESM configuration jobs, CMGRIACF or CMGRITSS, respectively.

     Note: This action helps ensure that records can be successfully inserted into the Monitor repository.

6. Verify that Data Mart users have UPDATE access to the DATAMART entity in the CACMGR resource class by checking the job output from CMGRIACF, CMGRITSS or CMGRIRAC job respectively, if you are running CA ACF2, CA Top Secret, or IBM RACF.

   Note: The Data Mart repository contains information about security events the ESM product generates and processes. Allow use of the Data Mart only by those people who already can view this information directly from the mainframe security system.

7. Verify that the CAI.CEIQLOAD library is APF-authorized.

   This step ensures that program ECARTINT, which resides in CAI.CEIQLOAD, is also APF-authorized. The Router does not initialize if it is executed from an unauthorized library.

   Note: If you specified a different CEIQLOAD data set during installation, verify that this data set if APF-authorized.

Chapter 5: Configuring CA LDAP Server and CA DSI Server

CA LDAP Server and CA DSI Server Configuration

CA LDAP Server and CA DSI Server provide an interface to perform security administration against CA ACF2 and CA Top Secret databases and provide the following functions:

- The capability to route security database requests to remote systems by communicating with a remote CA LDAP Server or CA DSI Server. This includes the following:
  - Modify and delete user requests through the Investigator
  - Read and write access through the Security Administration in Quick Links
- Access to manage policy that is written through the CA Chorus CA Compliance Manager interface.
- Access to simulation
- Access to Security Command Manager
- The ability to query the CA Compliance Manager repository for summary reports with regards to compliance management
- CIA Real-Time update process

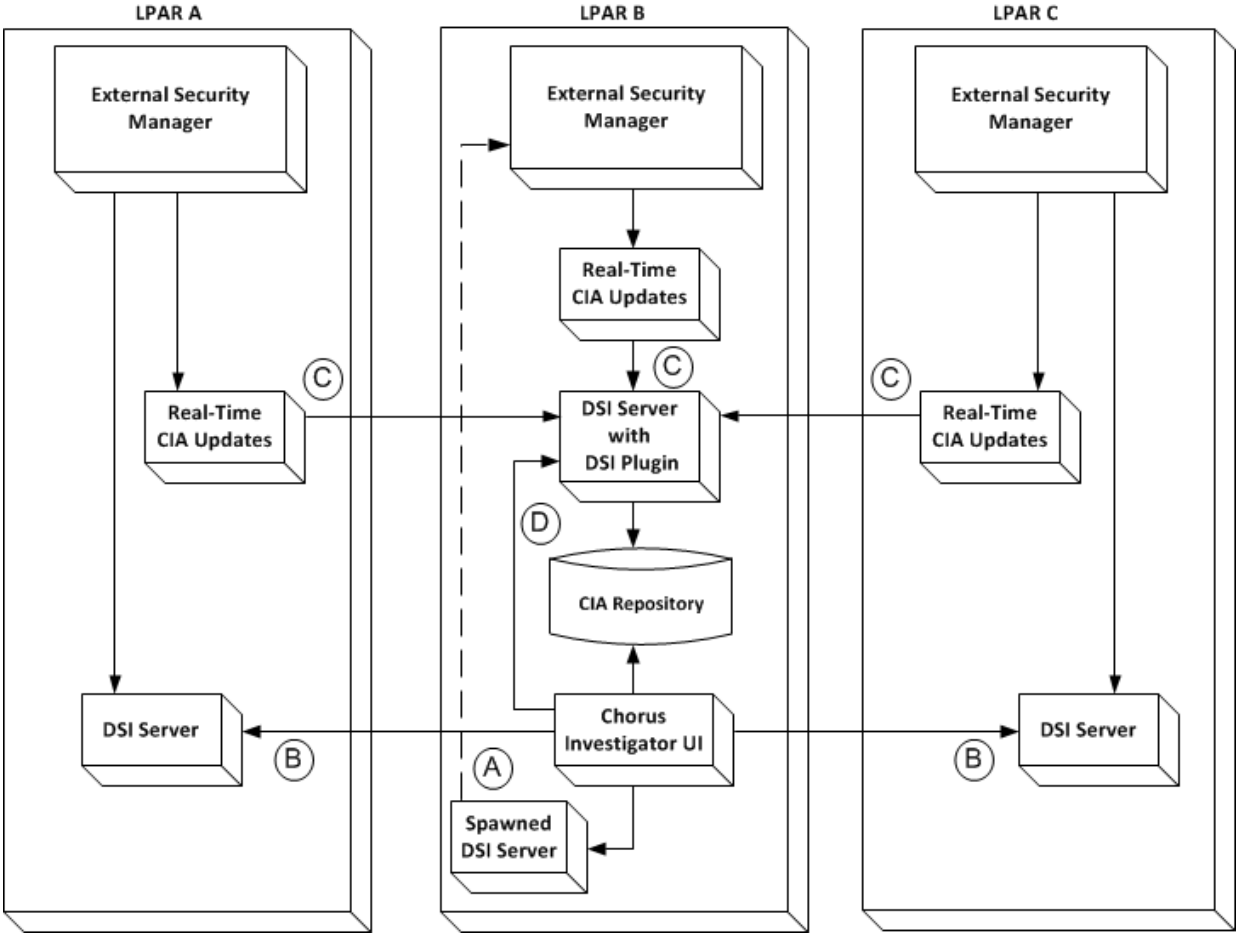
CA DSI Server provides a CA LDAP Server the capability of running security administration requests remotely to other LPARs. DSI also provides a mechanism to allow CA ACF2 or CA Top Secret running on local and remote computers to communicate to a single CIA repository.

Note: Detailed instructions are provided in the *CA LDAP Server Installation Guide* and *CA DSI Server Installation Guide*.

Sample CA DSI Server Configuration with CIA Real-Time

When the CIA real-time feature is enabled, the security product sends updates to CA DSI Server. CA DSI Server invokes the CA DSI Server plugin to send the update to the CIA repository. The result is that the CIA repository is updated and synchronized with the security product database. The CA DSI Server that is used for this process (spawned or standalone) must have the plugin configured. In this example, the CA DSI Server plugin is configured in the standalone CA DSI Server.

The following diagram shows a sample configuration with real-time CIA updates using standalone CA DSI Server servers:



This diagram shows a sample configuration for CIA real-time processing with the CA Chorus UI running on LPAR B. The CA Chorus UI gets data from the CIA repository, which communicates with the CA DSI Server. CA DSI Server receives real-time CIA updates from your external security manager (CA ACF2 or CA Top Secret).

- (A) CA Chorus Application Server spawns a CA DSI Server to perform authentication and resource checks on LPAR B.
- (B) LPAR A and C include a standalone CA DSI Server. The CA DSI Server plugin is not required for the CA DSI Servers on LPAR A and C.

When a user wants to execute a native command from CA Chorus, they launch the Security Command Manager and type in a command. CA Chorus sends the command to the CA DSI Server for execution and results. For this CA DSI Server to Security Command Manager interaction, the CA DSI Server is defined in data set member E1MI0015 in *your_chorussec_hlq*.CE1MJCL. See the CA Chorus *Installation Guide*.

- (C) CIA real-time updates from the security products on LPAR A and C are sent to the CA DSI Server running on LPAR B. The CA DSI Server feeding the CIA repository on LPAR B requires the CA DSI Server plugin. The CA DSI Server plugin is invoked to write updates to the CIA repository.

  Note: The Real-Time CIA updates are a sub-task of the external security manager, not a stand-alone STC.

- (D) Security Command Manager and simulation are executed from the CA Chorus interface on LPAR B point to the local system.

Obtain LDAP Configuration Values

The following CA LDAP Server values are required for the CA Compliance Manager interface installation procedure.

LPAR name or IP Address

Defines the name or IP address of the system running the CA LDAP Server.

Port number

Specifies the TCP/IP port that CA LDAP Server is using.

Example: 389

LDAP suffix

Specifies the values that let CA LDAP Server and CA Chorus for Security and Compliance Management communicate; these values identify the back-end.

Example: o=ca,c=us

Important! These values should have been obtained during installation of CA LDAP Server. If not, use the following procedure to obtain these values.

Follow these steps:

1. Obtain LDAP status values by issuing the following command from a z/OS console:

   ```
   F LDAPRnn,STATUS
   ```

   CA LDAP Server displays the LDAP port and its status.

2. Obtain LDAP back-end values by issuing the following command from a z/OS console:

   ```
   F LDAPRnn,BACKEND
   ```

   CA LDAP Server displays the LDAP suffix and current back-end values.

3. Use the output to identify and record the values that you need for the installation.

Example: Sample Output from the STATUS Command

The following is an example of output from the STATUS command. This command shows the LDAP port.

Note: You need the field in bold to complete the installation.

```
ETLDP05I CA LDAP Server status: 928
          slapd             15.2012.0229
          libslapd          15.2012.0229
          libsi             15.2011.1104
          back_cmdc_utf     15.2012.0305
          libsqlite3        15.2012.0229
          libmapres         15.2012.0229
          CADCPP32          14.00.0000
          back_cmgr_utf     15.2012.0305
          libsqlite3        15.2012.0229
          libmapres         15.2012.0229
          DSNAOCLI          DSN0601
          Security Product  ACF2 v15.0
          Debug Level       0
          Syslog Level      0
          Listeners         ldap://:1069 IP=(::):1069
                            ldap://:1069 IP=0.0.0.0:1069
          Enable Verify     No
          Auth Location     OS390
          Auth Source       CLIENT
          Auth Servers      none
          Auth Codeset      IBM-1047
          PT Appl Id        none
          PTReqr Id         none
          PTReqr PwFile     none
          Process ID File   "./conf/slapd.pid"
          Arguments File    "./conf/slapd.args"
          Max Threads       32
          Key Ring Name     none
          Cert Label        none
          Verify Clients    NEVER
```

Example: Sample Output from the BACKEND Command

The following is an example of output from the BACKEND command. This command shows you the LDAP suffix values that you need for the installation.

Note: You need the fields in bold to complete the installation.

```
ETLDP05I CA LDAP Server status: 935
      Status for cmgr_utf backend:
             suffix        o=cmgr,c=us
             DB Location   DSN0
             DB User       SYSADM1
             Tbl Qualifier CMGRQ1
             Policy DD     MAPDB
             Permit class  CIEM
             Permit entity CIEM
             DB Discovered Yes
             Adm Account   ADMACCOUNT
             Account Count 21
             Sec Control   SECCONTROL
             Control Count 15
             Adm Policy    ADMPOLICY
             Policy Count  21
             Adm Misc      ADMMISC
             Misc Count    19
             Obj Access    OBJACCESS
             Obj Acc Count 58
             Sys Access    SYSACCESS
             Sys Acc Count 20
             USS User      USSUSER
             User Count    32
             USS File      USSFILE
             File Count    32
             Header Delta  HDRDELTA
             Delta Count   13
             PDS Delta     PDSDELTA
             PDS Count     13
             List Delta    LSTDELTA
             List Count    26
             Single Delta  SNGDELTA
             Single Count  9
             Mulit Delta   MULDELTA
             Multi Count   4
             Chg Approval  CHGAPPROVED
             Chg App Count 10
```

```
Status for cmdc_utf backend:
       suffix        o=cmdc,c=us
       DB DSN        DATACOM
       DB User       DCOMUSER
       Tbl Qualifier CMGRD1
       Policy DD     MAPDB
       Permit class  CIEM
       Permit entity CIEM
       DB Discovered Yes
       Adm Account   ADMACCOUNT
       Sec Control   SECCONTROL
       Adm Policy    ADMPOLICY
       Adm Misc      ADMMISC
       Obj Access    OBJACCESS
       Sys Access    SYSACCESS
       USS User      USSUSER
       USS File      USSFILE
       Header Delta  HDRDELTA
       Delta Count   13
       PDS Delta     PDSDELTA
       PDS Count     13
       List Delta    LSTDELTA
       List Count    26
       Single Delta  SNGDELTA
       Single Count  9
       Mulit Delta   MULDELTA
       Multi Count   4
       Chg Approval  CHGAPPROVED
       Chg App Count 10
```

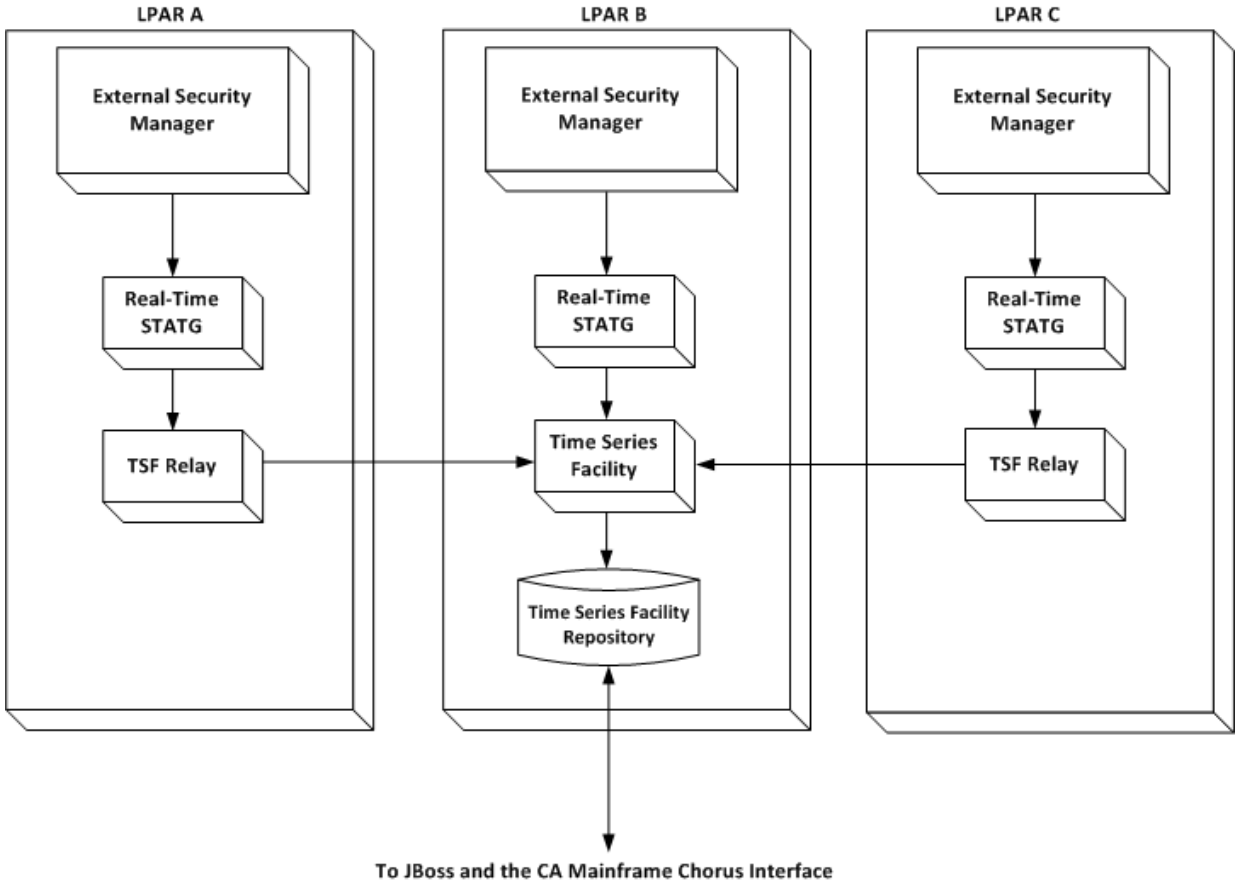
Chapter 6: Addressing Time Series Requirements

Provide Security Performance Data to TSF

The Time Series Facility (TSF) displays security performance data in CA Chorus. Before you can view this data using TSF, statistics gathering in CA ACF2 or CA Top Secret must be started. Statistics gathering is the process of collecting system statistics and sending data to TSF for a specific time frame, which is measured in seconds.

Note: For more information about activating real-time statistics gathering in CA ACF2, see the *CA ACF2 Administration Guide*. For more information about activating real-time statistics gathering in CA Top Secret, see the *CA Top Secret Control Options Guide*.

The following diagram shows a real-time statistical gathering (STATG) configuration for a single enterprise:



Your external security manager uses the following process to provide real-time statistical data to TSF:

- Checks to see whether real-time statistics are being gathered. If yes, data is passed to the TSF relay on remote systems and directly to TSF on the local system.
- Data is saved in the TSF repository.

Note the following:

- If you are sending data from CA ACF2 or CA Top Secret on a different LPAR than TSF, connect to TSF from the remote LPAR through the TSF Relay. For more information about the TSF relay, see the *CA Chorus Installation Guide*.
- The Real-Time STATG is a sub-task of the external security manager, not a stand-alone STC.

For more information about TSF, see the *CA Chorus Installation Guide*.

For CA ACF2

To view CA ACF2 metrics in CA Chorus, the STATG bit in the GSO record must be turned on and statistics must be enabled with the Start command. You must wait for the time interval setting before data displays in the metrics panel. Metrics display only when actions are occurring.

Note: The Time Series Facility must be active in order for records to appear in the metrics panel.

Follow these steps:

1. Specify the following options in the CA ACF2 CHORUS GSO record on each LPAR from which you want to send data to TSF:

   STATG

   Specifies to start statistics gathering in CA ACF2 for TSF.

   Default: NOSTATG

   STATGINT(15|nn)

   Specifies the time interval in seconds to capture statistical data that is routed to TSF.

   Valid values: 15, 30, 60, 300, 900, 1800, or 3600 seconds

   Default: 15

   Recommended setting: 30

2. Issue the following commands:

   ```
   ACF

   SET CONTROL(GSO)
     CONTROL
   INSERT CHORUS STATG STATGINT(30)
   ```

3. Issue the following commands to activate:

   ```
   F ACF2,REFRESH(CHORUS)
   ```

   Note: You can set additional options to identify the types of statistics you want to gather, define where statistics are written, and so on. For more information about these options, see the *CA ACF2 Administration Guide*. If CA ACF2 is restarted, statistical information is reset. If the STATG gathering task is deactivated using the STOP command, statistical information is not captured for TSF.

For CA Top Secret

To view CA Top Secret metrics in CA Chorus, the CHORUSSTATG(ON) control option must be set. You must wait for the time interval setting before data displays in the metrics panel. Metrics display only when actions are occurring.

Follow these steps:

1. Specify the following control options in CA Top Secret on each LPAR from which you want to send data to TSF:

   CHORUSSTATG(ON)

   Specifies to start statistics gathering in CA Top Secret for TSF.

   Default: OFF

   Important! Include CHORUSSTATG(ON) in the CA Top Secret parameter file so that it is available at CA Top Secret startup. Otherwise, statistical data gathering (STATG) in CA Chorus needs to be started manually.

   CHORUSSTATI(*nnnn*)

   Specifies the time interval in seconds to capture statistical data that is routed to TSF.

   Valid values: 15, 30, 60, 300, 900, 1800, or 3600.

   Default: 15

   Recommended setting: 30

   Note: You can set additional options to identify the types of statistics you want to gather, and so on. For more information about these options, see the *CA Top Secret Control Options Guide*.

2. Issue the following commands to activate:

   ```
   TSS MODIFY(CHORUSSTATG(ON))
   TSS MODIFY(CHORUSSTATI(30))
   ```

   Security performance data is provided to TSF.

Chapter 7: Implementing CIA Real-Time for CA Chorus for Security and Compliance Management

CIA and CA Chorus

CA Chorus for Security and Compliance Management leverages information from various sources. For many features, it interacts directly with the mainframe security product. For real-time processing of security events, it leverages the security event capabilities of CA Compliance Manager. For user (account) and security policy information, the CA Chorus security discipline processes information from a CIA repository.

The information in the CIA repository is accurate only at the time the batch unload and load process is performed. Any changes to the security database information after the information is unloaded are not reflected in the CIA repository.

The real-time nature of processing security and compliance information requires that information in the CIA repository is an accurate reflection of current information in the security product definitions. Any changes to the information in the security product database must be communicated in real time to the CA Chorus CIA repository. The CIA real-time feature helps ensure that the information in the CIA repository reflects the current information in the security product database.

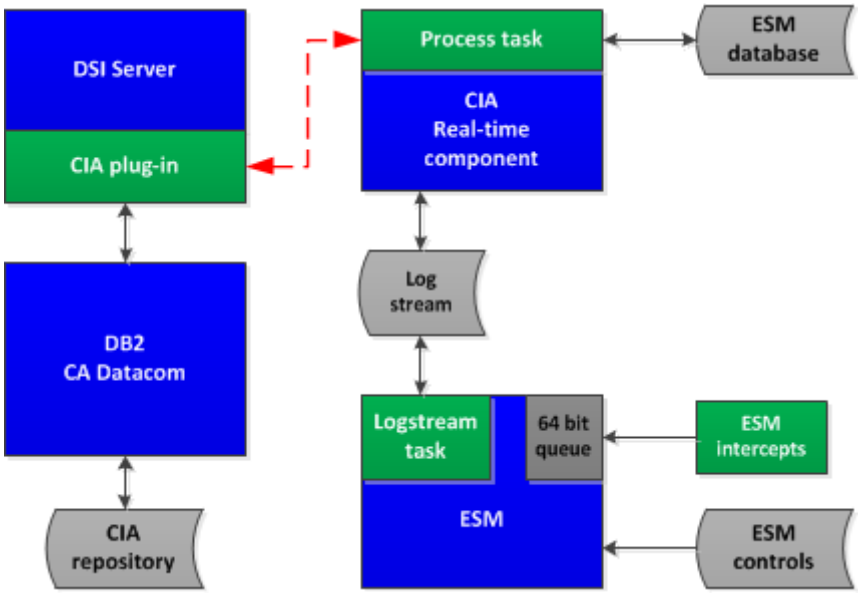
Note: The CIA real-time feature is available only when CA Chorus is installed at your site. When the CIA real-time feature is enabled, it performs an LMP check for the CA Chorus LMP key. Without the key, the CIA real-time feature cannot be enabled.

How CIA Real-Time Processing Works

CIA real-time processing helps ensure that the information in the CIA repository is updated as changes occur to the security product database. When it is enabled, the CIA real-time feature performs the following actions:

- A processing task in the security product address space removes the update requests from the request queue. The update request is written to a z/OS system logger logstream dedicated to the CIA real-time feature.
- A CIA real-time component reads the update requests from the CIA logstream. The component sends the request to a CA DSI Server running on the z/OS image where the CIA repository resides. When the CIA real-time feature is implemented, a CA DSI Server is required on the LPAR with the CIA repository. This CA DSI Server processes the CIA real-time requests, and updates the information in the CIA repository.
- A CIA real-time process in the CA DSI Server communicates the update requests to the DB2 or CA Datacom/AD subsystem where the CIA repository resides. The corresponding changes are made to the information in the CIA repository. The CA DSI Server communicates the results of the update request back to the CIA real-time component.
- If the update request was successfully processed into the CIA repository, the CIA real-time component deletes the update request from the CIA logstream.
- If the CIA real-time process was unable to complete due to a recoverable condition, the component stops processing, communicates the recoverable condition to the operator, and waits for resolution of the condition. The following are examples of these recoverable conditions:
  - The CA DSI Server communication path through TCP/IP is unavailable
  - The CA DSI Server is unavailable.
  - The CA Datacom/AD MUF or DB2 subsystem in which the CIA repository resides is unavailable
- If a logical error was encountered trying to update the security information, the CIA real-time component records the error condition in a journal file (if one was supplied). The CIA real-time component then deletes the update request from the CIA logstream. These logical errors usually indicate that the request could not be processed because the security information in the CIA repository does not reflect the information in the security product database. Some examples of these logical errors are:
  - The request is to add information that is already in the CIA repository.
  - The request is to update information that does not exist in the CIA repository.
  - The request is to delete information that does not exist in the CIA repository.

The following diagram illustrates the architecture of the CIA real-time process, and how the update requests flow from the security product to the CIA repository.



Implement the CIA Repository in CA Datacom/AD

If you implement the CIA security repository in CA Datacom/AD, execute the following steps:

- Create the CA Datacom/AD MUF
- Start the CA Datacom/AD MUF
- Link the CIA Functions with CA Datacom/AD
- Delete the CIA Repository in CA Datacom/AD (if required)
- Define the CIA Repository to CA Datacom/AD
- Implement CA Datacom/AD Server

Create the CA Datacom/AD MUF

Create and deploy a new and empty CA Datacom/AD Multi-User Facility (MUF) that holds the CIA repository. For more information, see the CA Datacom/AD *Installation Guide for z/OS*.

Follow these steps:

1. Edit and submit the CA Datacom/AD AXCUS00 job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job builds, populates, and mass-edits the installation JCL data set.

2. Edit and submit the CA Datacom/AD AXCUS01 job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job Includes all customization for the CIA CA Datacom/AD MUF.

3. Edit and submit the CA Datacom/AD AXNEW01 job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job allocates and populates data sets that the CIA CA Datacom/AD MUF needs.

4. Edit and submit the AXRIM01 job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job Installs the PC CALLS.

5. Edit and submit the AXAPFADD job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job provides a CA SYSVIEW example to dynamically add libraries to be APF listed.

6. Edit and submit the AD14STRT job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job is the procedure that starts the CA Datacom/AD MUF.

   The AD14STRT job can also be used to create the MUF as a started task procedure. For more information, see Create the CA Datacom/AD MUF for CIA as a Started Task Procedure (see page 99).

7. Edit and submit the AXIVP01 job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This is a sample install verification job.

8. Edit and submit AD14STOP job.

   Follow the instructions in the job for modifying. Verify that the job ran successfully.

Create the CA Datacom/AD MUF for CIA as a Started Task Procedure

Use the following procedure to create the CA Datacom/AD MUF for CIA as a started task procedure.

Follow these steps:

1. Follow the documented CA Datacom/AD rules on how to modify a JCL job to create the MUF as a started task procedure.
2. Copy the AD14STRT job from *your_datacom_hlq*.INSTJCL into the z/OS system procedure library where the CIA real-time component is executed.
3. Rename the AD14STRT job as the CA Datacom/AD MUF that you recorded in your Site Preparation Worksheet. For example, CIAMUF.
4. The installed CA Datacom/AD MUF must use the settings from AXDATIN1 and AXDATIN2, which contain initialization parameters, and reside in one of the following libraries:

   CA ACF2 - CAI.CAX1OPTN

   CA Top Secret - CAI.CAK0OPTN

   Important! DO NOT change the values for these initialization parameters unless requested to do so by CA technical support.

5. Copy the AXDATIN1 and AXDATIN2 members from the installation data set to a library you choose.
6. Modify the CA Datacom/AD MUF started task procedure to reference the location of the AXDATIN1 and AXDATIN2 members.

Start the CA Datacom/AD MUF for CIA Real-Time

The CA Datacom/AD MUF must be executing before the CIA repository can be defined.

Follow these steps:

1. Issue the following console command to start the CA Datacom/AD MUF, if not yet started.

   ```
   'S CIAMUF'
   ```

   Note: If you created a MUF with a name that is different than the recommended default, CIAMUF, use the correct MUF name in the command.

2. Verify that the CIAMUF successfully started.

Note: For complete information about executing the CA Datacom/AD MUF, see the CA Datacom/AD *Installation Guide for z/OS*.

Link the CIA Functions with CA Datacom/AD

Before the CIA application and repository can be defined in CA Datacom/AD, the CIA service function modules must be linked with CA Datacom/AD entry modules, and the resulting load modules must be available in the CA Datacom/AD MUF.

The CIALINKC job links CIA service function modules with CA Datacom/AD entry modules.

Follow these steps:

1. Edit the CIALINKC job in one of the following libraries:

   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and the Customization sections of the job to customize the job for your environment.

2. Submit the job.

   The job runs and completes.

3. Verify the output of the CIALINKC job.

   The CIA modules are successfully linked with the CA Datacom/AD entry modules.

Delete the CIA Repository for CA Datacom/AD (If Required)

An existing CIA repository for CA Datacom/AD must be deleted so that it can be redefined. The CIADCOMD job deletes an existing CIA repository.

Follow these steps:

1. If you have an existing CIA CA Datacom/AD repository, edit the CIADCOMD job in one of the following libraries:
   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and the Customization sections of the job to customize the job for your environment.
2. Submit the job.

   The job runs and completes.
3. Verify the output of the CIADCOMD job.

   The existing CIA CA Datacom/AD repository is successfully deleted.

Define the CIA Repository to CA Datacom/AD

The CIADCOM job performs the tasks of defining the CIA application and repository to CA Datacom/AD. Within the job are individual job steps that perform the following:

- Allocate the data sets to hold the CIA repository database.
- Define the CIA database to the CA Datacom/AD data dictionary.
- Initialize the CIA database
- Import the CIA database table and index definitions
- Import the application plans for the CIA service functions and procedure
- Create the CIA service functions and procedure

Follow these steps:

1. Edit the CIADCOM job in one of the following libraries:
   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and Customization sections of the job to customize the job for your environment.

2. Submit the job.

   The job runs and completes.

3. Verify the output of the CIADCOM job.

   The CIA application and repository are defined correctly in CA Datacom/AD.

Implement CA Datacom/AD Server for CIA

If you are implementing a CA Datacom/AD repository for CIA, configuration of the CA Datacom/AD Server is required for the following reasons:

- Enable PassTicket authentication (see PassTicket Configuration to Connect to Datacom/AD (see page 68))
- Provide a gateway from the JDBC and ODBC drivers to the <dd> CIA MUF
- Allow CA Datacom/AD Server to access the CIA repository in the CA Datacom/AD MUF for CIA

Important! The CA Datacom/AD Server must be implemented on the same LPAR as the CA Datacom/AD MUF containing the CIA repository.

Create the CA Datacom/AD Server Procedure for CIA

After creating and deploying the CA Datacom/AD Server, use the following procedure to create the CA Datacom/AD Server started task procedure.

Follow these steps:

1. Follow the documented CA Datacom/AD rules on how to modify a JCL job to create it as a started task procedure.
2. Copy the sample JCL job from the CA Datacom/AD Server installation data set to the library from which it is executed as a started task procedure and name the procedure appropriately. For example, CIASRV.
3. Edit the sample JCL job to create the new started task procedure (CIASRV). Conform the procedure to your installation standards and match the values in the CA Datacom/AD installation data sets that were used to create the CA Datacom/AD MUF for CIA.
4. Add the *your_chorus_hlq*.CETJPLD target library from the CA Chorus platform installation to the STEPLIB concatenation in the procedure.
5. Verify that all libraries that are in the STEPLIB concatenation of the procedure are APF-authorized.

Configure CA Datacom/AD Server to Connect to CA Datacom/AD for CIA

After deploying the CA Datacom/AD Server, perform the following procedure to configure the CA Datacom/AD Server to connect to the MUF for CIA.

The CA Datacom/AD parameters for CIA are located in the CIASRVP and HEAPCHK members in one of the following libraries:

CA ACF2 - CAI.CAX1OPTN

CA Top Secret - CAI.CAK0OPTN

Note: For more information about implementing the CA Datacom/AD Server, see the CA Datacom/AD Server *User Guide*.

Follow these steps:

1. Copy the CIASRVP and HEAPCK members to a library you choose.
2. Modify the CA Datacom/AD Server started task procedure (for example, CIASRV) to reference the location of the CIASRVP and HEAPCK members.
3. If you are using a separate MUF for the CIA repository than the one for CA Compliance Manager (recommended), ensure that the initialization parameters (in CIASRVR) for the CA Datacom/AD Server for CIA have the following values:

   ```
   SERVERNAME=CIAx_SYSy
   APPLID=CIAx_SYSy
   PLANNAME=$MBH
   AUTHID=SYSUSR
   PROTOCOL=BOTH
   TCPIP_HOST=LPARNAME
   DBUSERS=100
   TIMEOUT=6
   TIMEOUTWAIT=10
   LOGON=YES
   CHORUSEXT=CHRCXT10
   ```

4. If you are using the same MUF for the CIA repository and CA Compliance Manager repositories (sharing a MUF), ensure that the initialization parameters for the CA Datacom/AD Server for CIA have the following values:

   Important! The CA Datacom/AD Server initialization parameter values for CIA must be the same as the CA Datacom/AD Server initialization parameter values for CA Compliance Manager.

   ```
   SERVERNAME=CMGRx_SYSy
   APPLID=CMGRx_SYSy
   PLANNAME=$MBH
   AUTHID=SYSUSR
   PROTOCOL=BOTH
   TCPIP_HOST=LPARNAME
   DBUSERS=100
   ```

```
TIMEOUT=6
TIMEOUTWAIT
LOGON=YES
CHORUSEXT=CHRCXT10
```

Start CA Datacom/AD Server of the CA Datacom/AD MUF for CIA

After the CA Datacom/AD MUF is started and the CA Datacom/AD Server is configured, CA Datacom/AD Server must be started for the CA Datacom/AD MUF for CIA.

Follow these steps:

1. Start the CA Datacom/AD Server by issuing a console command to execute the started task procedure. For example:

   ```
   'S CIASRV'
   ```

   Note: If you created the CA Datacom/AD Server started task procedure with a name that is different than the recommended default, CIASRV, use the correct started task procedure name in the command.

2. Verify that the CA Datacom/AD Server was successfully started.

Note: For more information about starting CA Datacom/AD Server, see CA Datacom/AD Server *User Guide*.

Implement the CIA Repository in DB2

If you choose to implement the CIA security repository in DB2, execute the following steps:

- Create the DB2 subsystem
- Set up Workload Manager (WLM) and Resource Recovery Attach Facility (RRSAF)
- Start the DB2 subsystem
- Link the DB2 functions into modules
- Delete the CIA repository for DB2 (if required)
- Define the CIA repository in DB2

Create the DB2 Subsystem

For information about creating and deploying a DB2 subsystem, see the appropriate IBM DB2 documentation.

Follow these steps:

1. Check your Site Preparation Worksheet to verify the name of the DB2 subsystem you are using to hold the CIA repository.
2. Create and deploy the DB2 subsystem that holds the CIA repository.

Set Up Workload Manager (WLM) and Resource Recovery Attach Facility (RRSAF)

The CIA repository processing requires a set of CIA user-defined functions and a stored procedure. The CIA user-defined functions and stored procedure run in a Workload Manager (WLM) environment in DB2.

Operating environment setup is required for running user-defined functions and stored procedures in DB2.

Follow these steps:

1. If you have not set up your DB2 environment to use WLM-established address spaces, see the *IBM Redbook, DB2 for z/OS Stored Procedures: Through the CALL and Beyond* for directions on setting up WLM and RRSAF for this purpose.

   Note: We recommend that you set up a separate WLM environment for the CIA user-defined functions and stored procedure. This WLM procedure should have a NUMTCB value between 20 and 40. See the IBM Knowledge Center documentation *Managing DB2 Performance*.

2. Start RRASF on the z/OS system by issuing a console command that executes the procedure. For example:

   ```
   S RRS
   ```

Start the DB2 Subsystem

The DB2 subsystem must be executing before the CIA repository can be defined.

Follow these steps:

1. Verify that RRASF is running, before starting the DB2 subsystem.
2. Start the DB2 subsystem by issuing a console command that executes the procedure. For example:

   ```
   +DSNCSTART DB2
   ```

3. Verify that the DB2 subsystem successfully started.

Note: For more information about executing the DB2 subsystem, see the appropriate IBM DB2 documentation.

Link the DB2 Modules into Functions

For the service functions to operate properly, link the DB2 modules, DSNRLI and DSNTIAR, into the service functions in the target DB2 subsystem with the security repository.

Follow these steps:

1. Edit the CIA4LNK1 job in one of the following libraries:
   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Modify the job to conform to your installation standards and direct it to the target DB2 subsystem. Follow the instructions in the Notes and Customization sections of the job to customize the job for your environment.
2. Submit the job.

   The job runs and completes.
3. Verify the output of the job.

   The CIA modules are linked.

Delete the CIA Repository for DB2 (If Required)

An existing CIA repository for DB2 must be deleted so that it can be redefined. The CIADB2D job deletes an existing CIA repository for DB2.

Follow these steps:

1. Verify that the DB2 subsystem into which the CIA repository is installed is running.

   If you have an existing CIA DB2 repository, edit the CIADB2D job in one of the following libraries:

   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and the Customization sections of the job to customize the job for your environment.

2. Submit the job.

   The job runs and completes.

3. Verify the output of the CIADB2D job.

   The existing CIA DB2 repository is successfully deleted.

Define the CIA Repository for DB2

The CIADB2 job performs the tasks of defining the CIA application and repository to DB2. Within the job are individual job steps that do the following:

- Define the CIA database, table spaces, tables, and indexes that comprise the security repository.
- Define the CIA service functions
- Define the CIA stored procedures
- Bind the application packages that correspond to the service functions

Note: If you are an existing CIA user, the CIADB2 combines a number of separate jobs (CIADDL, CIAFUNC, CIAPROC, and CIABIND) that were run with previous CIA releases.

Follow these steps:

1. Verify that the DB2 subsystem into which the CIA repository will be installed is running.
2. Edit the CIADB2 job in one of the following libraries:
   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Modify the job to conform to your installation standards and direct it to the target CIA DB2 subsystem where you want to define the repository.
3. Submit the job.

   The job runs and completes.
4. Verify the output of the CIADB2 job.

   The CIA application and repository are defined correctly in DB2.The DB2 data structures are defined.

Configure CA DSI Server for CIA Real-Time

CA DSI Server provides a remotely callable interface that uses TCP/IP to allow applications anywhere within the enterprise to communicate with the mainframe ESMs. After you have defined the CIA repository, functions, and stored procedure in the DB2 subsystem or CA Datacom/AD MUF, configure and implement the CA DSI Server that is used for the CIA real-time process on the z/OS image with the DB2 subsystem or CA Datacom/AD MUF.

Follow these steps:

1. On the z/OS image where the CA Chorus CIA repository resides, manually edit the dsi.conf configuration file using oedit or vi editor.

   Note: The dsi.conf file can be found in the directory where CA DSI Server was installed. (Default location: /usr/lpp/caldapr151)

2. If you are using a CIA DB2 repository:

   - Add the following lines in uppercase to the end of the dsi.conf file

     ```
     PLUGIN CIADSMOD MODULE CIADSMOD
     DBTYPE DB2
     DB2SSID ssid
     DB2PLAN CIADSREQ
     ```

   - Replace ssid with the CIA subsystem name or group attachment name that the CIA real-time plugin connects
   - Enter the ssid in uppercase. For example, DSNC.

     If SDSNLOAD is not in the linklist, add it to the STEPLIB for the CA DSI Server started task (dsi.env).

     For example:

     ```
     //STEPLIB DD DSN=DSN910.SDSNLOAD,DISP=SHR
     ```

     Note: Enter all fields in uppercase.

3. If you are using a CIA CA Datacom/AD repository:

   - Add the following lines in uppercase to the end of the dsi.conf file

     ```
     PLUGIN CIADSMOD MODULE CIADSMOD
     DBTYPE DATACOM
     DCOMMUF mufname
     ```

   - Replace mufname with the CIA subsystem name or group attachment name that the CIA real-time plugin connects. CA Datacom/AD displays this value in the joblog at MUF startup in MUFNAME=.

     Note: Add the CA Datacom/AD CUSLIB and CAAXLOAD to the STEPLIB concatenation for the CA DSI Server started task (DSIR15).

     For example:

     ```
     //STEPLIB DD DSN=DATACOM.CUSLIB,DISP=SHR
     //STEPLIB DD DSN=DATACOM.CAAXLOAD,DISP-SHR
     ```

   - Enter the mufname in uppercase. For example, CIAMUF.

Begin the CIA Real-Time Recording

The following steps prompt the security product to begin recording changes made to security product information that is replicated in the CIA repository.

- Define the CIA Real-Time Logstream (see page 110)
- Allow Recording of Update Requests to the CIA Logstream (see page 113)

Important! Perform the following steps on every z/OS image whose security information is represented in the CA Chorus CIA repository. If a security product database is shared across multiple z/OS images, perform these tasks on each of the z/OS images. Administrative commands, SAF calls, and user sign-on and signoff processes on any of the z/OS images can change information in the security database that is replicated in the CIA repository. The CIA real-time process must communicate all of these changes to the CIA repository.

Define the CIA Real-Time Logstream

The CIA real-time feature uses a dedicated z/OS system logger logstream to record update requests made to any security product information that is replicated in the CIA repository. The CIA real-time component reads this logstream and communicates the update requests to the CIA repository.

Note: A separate and unique logstream is required for each z/OS image.

The CIALOGST job defines the logstream as DASDONLY(YES), AUTODELETE(NO), and RETPD(0). This is intended to keep the offloaded data maintained by z/OS system logger to a minimum. The z/OS system logger is prevented from deleting any event records that it has offloaded that the CIA real-time component has not marked as deleted. These values can be changed per your installations requirements.

The size required for the logstream depends on a number of factors. Under normal processing, the life of any given record in the logstream is measured in seconds or less. The record is marked deleted as soon as the CIA database update has been completed. A minimal number of active records is present in the logstream, and any offloaded data is marked deleted by the CIA real-time process. However, two situations exist where this does not occur.

- During the initial implementation, the time that elapses between when the security product begins recording update requests into the logstream and when the CIA real-time component is started. For that duration, update requests are carried in the logstream without being processed and deleted.

- When any of the components in the CIA real-time process communication path are unavailable, the update requests remain in the logstream until the process path is restored. The components in the communication path are:
  - CIA real-time component
  - TCP/IP
  - CA DSI Server
  - CIA subsystem with the CIA repository

We recommend that you evaluate your network and system stability and the effort involved to reload the CIA repository information. If the time involved in the situations described is greater than the size of the logstream allows, the logstream fills up and update requests are lost. In this case, the security information in the CIA repository for this system must be deleted and repopulated. If this occurrence is likely and the effort involved is great, increase the size of the logstream accordingly.

Each block on the logstream contains a single event record and is 4096 bytes long. The number of records which the logstream can hold has an initial value of 1000 ('(STG_SIZE(1000)'). Increasing this number increases DASD space requirements and reduces the number of offloads performed by the z/OS system logger. Decreasing the number has the opposite effect. Because each system is different, it is important to monitor the number and frequency of offloads and balance it with the performance impact an offload can cause.

The definition of the parameters discussed and the various options and considerations for allocating and managing z/OS system logger logstreams can be found in the IBM Redbook System Programmer's Guide to: z/OS System Logger (SG24-6898-01).

Follow these steps:

1. Edit the CIALOGST job in one of the following libraries to define the CIA real-time feature logstream:
   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and the Customization sections of the job to customize the job for your environment.
2. Submit the CIALOGST job.

   The job runs and completes.
3. Verify the output of the CIALOGST job.

   The CIA logstream is successfully defined.

Allow Recording of Update Requests to the CIA Logstream (CA ACF2)

The GSO CHORUS record was created as part of the CIARTACF job that defines the CIA real-time security requirements. After the CHORUS record is updated, issue the following CA ACF2 commands to start the CIA real-time recording:

```
F ACF2,REFRESH(CHORUS)
F ACF2,CIA(START)
```

Define CIA Real-Time Control Options (CA Top Secret)

The CA Top Secret control options provide the information required by the CIA real-time component to connect to the DSI server and to read and process the update requests from the CIA logstream.

When specified, the following fields in the CA Top Secret control options enable the recording of update requests to the CIA logstream.

- CIART(ACTIVE)
- CIALOGNAME(*log stream name*)
- CIAMAXSTOR(25|*nnn*)
- CIAHOST(*CIA DSI host name*)
- CIAPORT(*nn*)

Follow these steps:

1. Modify the CA Top Secret control options to enable recording of update requests to the CIA logstream.
2. Edit the CA Top Secret parameter file to make changes permanent.

Note: For more information about these control options, see the *CA Top Secret Control Options Guide and the CA Top Secret Compliance Information Analysis Guide*.

CIAAUTO(START|NOSTART)

Specifies whether CA Top Secret will automatically start the CIA real-time component started task during CA Top Secret initialization. .

CIAHOST(*CIA DSI host name*)

Specifies the 1-to-255 character host name for the CA DSI Server on the z/OS image that hosts the CIA repository.

CIALOGNAME(*log stream name*)

Specifies the name of the log stream used by the CIA real-time process.

CIAMAXSTOR(25|*nnn*)

Specifies the maximum amount of above the bar (64 bit) storage in the CA Top Secret address space that is used to temporarily hold the queue of update requests that are waiting to be written out ot the CIA logstream.

CIAPORT(*nn*)

Specifies the port number for the CA DSI Server on the z/OS image that hosts the CIA repository.

CIAPROCNAME(*CIA started procedure name*)

Specifies the procedure name for the CIA real-time component started task procedure.

CIART(ACTIVE|INACTIVE)

Specifies whether the CIA real-time feature is active or inactive. The default is INACTIVE.

CIASYSID(*CIA sysid used in the CIA database*)

Specifies the SYSID parameter value that was used for this security image when its information was loaded into the CIA repository.

This option allows multiple z/OS images to update a single security image in CIA. When a security product database is shared across multiple z/OS images, each of those images must use the CIASYSID control option to specify the SYSID of the single image that was unloaded.

Allow Recording of Update Requests to the CIA Logstream (CA Top Secret)

CIA real-time recording may have been activated during the procedure to define the control options in Define CIA Real-Time Control Options (CA Top Secret) (see page 112). If not, issue the following command:

```
F TSS,CIART(ACTIVE)
```

Estimate Storage Requirements for the Unload Data Set (CA ACF2)

If you are using CA ACF2, estimate the amount of space (in cylinders) that is required to allocate the Unload utility data set. See the CA ACF2 Worksheet (see page 115).

Follow these steps:

1. Estimate the number of records in your site's CA ACF2 security databases for the following:
   - users (logonids, user profiles, and user-defined fields)
   - rules (data set rules, resource rules, and CIA resource rules)
   - rule lines

   Important! If you are adding user-defined fields to the UNLOAD file, multiply the total count of user-defined fields represented by the CIA Unload Utility SYSIN file USERFIELD input control statements by the total number of number of logonids. For example, if there are 10 users, and 10 user-defined fields in the ACFFDR, the total count would be 100. The number of user records generated by adding user-defined fields significantly increases the size of the UNLOAD file that needs to be allocated.
2. Multiply the total count of each of these records by the multiplication factor provided in the following worksheet to calculate the total space (in bytes) required for each type of record.
3. Divide the total number of bytes needed for each of these types by the number of bytes on a cylinder for the hardware disk model you are using. This way you determine the total number of cylinders of space to allocate for each type.

   Note: IBM disk model 3390 has 849,960 bytes per cylinder, which is the number provided in the following worksheet.
4. Add the number of cylinders of space needed for each type of record to calculate the total space (in cylinders) to allocate for the UNLOAD data set.

   The space allocation calculated may be more than your site actually requires. The multiplication factors provided in the following worksheet are based on maximum record lengths for target tables in the UNLOAD data set. After you run the Unload utility one time, you know exactly how much space was used in the UNLOAD data set. Then release any unused space in the UNLOAD data set or reallocate the UNLOAD data set with the desired space allocation and rerun the Unload utility.

CA ACF2 Worksheet

Use the following worksheet to calculate the necessary space requirements for the UNLOAD data set in CA ACF2.

Calculation of Space Allocation for UNLOAD Data Set

User Records

Use the following to calculate the total space for user records.

1. Number of logonid records: _____
2. Number of user-defined fields: _____

   Note: Skip this line if the user-defined fields are not being implemented.
3. Total number of user-defined records: _____

   Multiply the number of user-defined fields in the ACFFDR by number of logonid records.

   Note: Skip this line if the user-defined fields are not being implemented.
4. Total number of profile records: _____
5. Total number of user records: _____

   Add total number of user-defined records, or if user-defined fields are not being implemented, add the number of logonid records to the number of user profile records.
6. Total space (bytes) needed for user records:

   Multiply total number of user records by 15,796 bytes.
7. Total space (cylinders) needed for user records: _____

   Divide total space (bytes) needed for user records by 849,960 bytes/cylinder.

Rule Records

Use the following to calculate the total space for rule records.

1. Number of rules (data set, resource, and DB2): _____
2. Total space (bytes) needed for rules: _____

   Multiply number of rules by 483 bytes.
3. Total space (cylinders) needed for rules: _____

   Divide total space (bytes) needed by rules by 849,960 bytes/cylinder.

Rule Lines

Use the following to calculate the total space for rule lines.

1. Number of rule lines (data set, resource, and DB2): _____
2. Total space (bytes) needed for rule lines: _____

   Multiply number of rule lines by 1,897 bytes.
3. Total space (cylinders) needed for rule lines: _____

   Divide total space (bytes) needed for rule lines by 849,960 bytes/cylinder.

Control Records

Use the following to calculate the total space for control records.

1. Number of control records (DCO): _____
2. Total space (bytes) needed for control records:_____

   Multiply number of control records by 1,990 bytes.
3. Total space (cylinders) needed for control records: _____

   Divide total space (bytes) needed for control records by 849,960 bytes/cylinder.

Total Space Needed for UNLOAD Data Set

1. Total space (cylinders) needed for unload data set: _____

   Add the total space (cylinders) for each type of record to calculate the total space required for the Unload data set.

Estimate Storage Requirements for the Unload Data Set (CA Top Secret)

If you are using CA Top Secret, the following explains how to estimate the amount of space (in cylinders) to allocate the UNLOAD utility data set. See the CA Top Secret Worksheet (see page 117).

To estimate the necessary amount of space

1. Estimate the number of records in your site's CA Top Secret security file for ACIDS, owned resources, and user-defined fields.
2. Multiply the total count of each of these records by the multiplication factor provided in the following worksheet to calculate the total space (in bytes) required for each type of record.

3. Divide the total number of bytes needed for each of these types by the number of bytes on a cylinder for the hardware disk model you are using.

   You have calculated the total number of cylinders of space to allocate for each type of record.

   Note: IBM disk model 3390 has 849,960 bytes per cylinder, which is the number provided in the following worksheet.

4. Add the number of cylinders of space needed for each type of record

   You have calculated the total space (in cylinders) to allocate for the UNLOAD data set.

Note: The space allocation calculated may be more than your site actually requires. The multiplication factors provided in the following worksheet are based on maximum record lengths for target tables in the UNLOAD data set. After you run the unload utility one time, you will know exactly how much space was used in the UNLOAD data set, and can then release any unused space in the UNLOAD data set or reallocate the UNLOAD data set with the desired space allocation and rerun the unload utility.

CA Top Secret Worksheet

Use the following worksheet to calculate the necessary space requirements for the UNLOAD data set in CA Top Secret.

Calculation of Space Allocation for UNLOAD Data Set

Number of user records (ACIDS and profiles):		_____ records (1)
_____	(1) x 15,796 bytes =	
	Total space needed for user records:	_____ bytes (A)
_____	(A) / 849,960 bytes/cylinder=	
	Total space needed for user records:	_____ cylinders(AA)

Calculation of Space Allocation for UNLOAD Data Set

Number of owned resources:		_____ rules(2)
_____	(2) x 483 bytes=	
	Total space needed for rules:	_____ bytes (B)
_____	(B) / 849,960 bytes/cylinder=	
	Total space needed for rules:	_____ cylinders (BB)

Calculation of Space Allocation for UNLOAD Data Set

Add lines (AA) and (BB) to calculate the total space required for all types.

Total space needed for unload data set: _____ cylinders

Allocate the Unload Data Set

After you have calculated the storage requirements for the UNLOAD data set, allocate the data set.

Follow these steps:

1. Edit the CIAALLOC job in one of the following libraries:
   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Change the job to include the necessary space allocation to conform to your installation standards.

   The UNLOAD data set is allocated as physical sequential (PS) with a variable-length (VB) record format, and a record length of 3157 (the maximum record length of a target table).
2. Submit the job.

   The job runs and completes.
3. Verify the output of the CIAALLOC job.

   The UNLOAD data set is allocated.

Unload the Security Information

The CIAUNLD job executes the unload utility, which reads the security information from the security database and creates an unload data set. The unload data set contains load data in DB2 format which is used to populate the CIA repository.

All CIA repositories (DB2 and CA Datacom/AD) use the same unload process. The process for loading the security data into the CIA repository differs slightly, depending on whether you are using DB2 or CA Datacom/AD for the CIA repository.

The information from the security database must be unloaded into a target data set (UNLOAD). The UNLOAD data set must be defined and allocated before it can be used.

The following tasks unload the security information from the security database:

- Verify authorization to run the TSSFAR utility (CA Top Secret only)
- Run TSSFAR utility (CA Top Secret only)
- Run the CIACFILE job (CA Top Secret only)
- Verify authorization to run the CIA Unload utility
- Implement user-defined fields
- Run the CIA Unload utility
- Check the output from the UNLOAD utility

To replicate the most current information in the CIA repository, these tasks should be performed in the order specified each time you incorporate changes made to the security file.

Run TSSFAR Utility (CA Top Secret Only)

TSSFAR can be used to validate the security file for CIA.

Follow these steps:

1. From your current release of CA Top Secret, run the TSSFAR utility with the SFSTATS option against your existing backup security file. A file analysis report is generated.
2. Use the file analysis report to verify that all the security data can be successfully unloaded to the unload utility UNLOAD file.

Important! Running TSSFAR against the security file can cause degradation to system performance. We recommend that TSSFAR always runs against a backup file.

Run the CIACFILE Job (CA Top Secret Only)

The CIACFILE job executes TSSCFILE. The TSSCFILE output is used as input into the CIA Unload Utility to generate data to be loaded into a DB2 or CA Datacom/AD CIA database.

Follow these steps:

1. Edit the CIACFILE job in CAI.CAK0JCL0.

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and the Customization sections of the job to customize the job for your environment.

2. Submit the job.

   The job runs and completes.

3. Verify the output of the CIACFILE job.

   The TSSCFILE data is generated.

   Important! The CIACFILE job attempts to list several record types (TIMEREC, CALENDAR, KERBLINK, and EIMPROF) that may not exist in your security file and results in a return code 8. Ignore these erros if you do not utilize these record types.

Verify Authorization to Run the CIA Unload Utility

Verify that you have authorization to run the CIA Unload utility.

Note: These authorizations should already have been permitted during the process of defining the security requirements for the CIA real-time component.

- CA ACF2 checks for and allows only users who have an unscoped SECURITY attribute in their logonid to run the Unload utility.
- CA Top Secret checks for and allows only users who have an unscoped SECURITY attribute in their ACID to run the unload utility.

Implement User-Defined Fields

If your site has defined its own user fields on the logonid record for CA ACF2 or ACID for CA Top Secret, you can include this information in the CIA repository.

The CIAUNLD job executes the unload utility, which reads information from the security database and creates an unload data set. The unload data set contains load data (in DB2 format) that populates the CIA repository.

To include specific user-defined fields, you can specify USERFIELD input control statements in the SYSIN file of the CIAUNLD job (to generate USER-DEFINED FIELD table records containing the field data). To review the specific user-defind field tables, see the CIA Data Dictionary and Data Model in the CA ACF2 or CA Top Secret *Compliance Information Analysis Guide*.

Note: By default, the SYSIN file specifies to add all user-defined fields. If you do not want to include user-defined field data in the repository, specify the USERFIELD(*NONE*) input control statement in the CIAUNLD job.

Example: Add User-Defined Fields FIELD1, FIELD2, and FIELD3

The following unload utility SYSIN input control statements specify three user-defined character type fields (FIELD1, FIELD2, and FIELD3):

```
//SYSIN DD *
USERFIELD(FIELD1)
USERFIELD(FIELD2)
USERFIELD(FIELD3)
/*
```

These USERFIELD control statements instruct the CIA unload utility to process FIELD1, FIELD2, and FIELD3 (when found) and generate UDFCHAR records in the UNLOAD data set.

Example: Do Not Implement User-Defined Fields

The following unload utility SYSIN input control statement specifies to omit user-defined fields:

```
//SYSIN DD *
USERFIELD(*NONE*)
/*
```

Example: Implicitly Add All User-Defined Fields

The following unload utility SYSIN file implicitly specifies to add all user-defined fields (because no USERFIELD input control statements exist). This specification is the default specification.

```
//SYSIN DD *
/*
```

Example: Explicitly Add All User-Defined Fields

The following unload utility SYSIN input control statement explicitly specifies to add all user-defined fields:

```
//SYSIN DD *
USERFIELD(*ALL*)
/*
```

Run the CIA Unload Utility

The CIAUNLD job executes the Unload utility, which reads the security information from the security database and creates an unload data set. This unload data set is used as input to the load process.

Note: A number of control statements control the processing of the Unload utility. These statements can be specified as input to the SYSIN input data set.

Follow these steps:

1. Edit the CIAUNLD job in one of the following libraries:
   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Specify the Unload data set allocated earlier and any input control statements that you require to conform to your site's standards.

   Important! For complete information about required and optional input control statements, see the CA ACF2 or CA Top Secret *Compliance Information Analysis Guide*.

2. Specify one of the following values if you do not want to unload all user-defined fields in your security database,

   USERFIELD(*NONE*)

   Specifies no user-defined fields will be unloaded.

   USERFIELD(*fieldname*)

   Specifies an external user-defined field name that you want to add to the CIA repository.

   Note: Specify one USERFIELD(*fieldname*) input control statement for each user-defined field you want to unload.

3. Submit the job.

   The job runs and completes.

4. Verify the output of the CAIUNLD job.

   Verify that the utility completed successfully. If the CIAUNLD job fails for any reason, run the job again until it successfully completes. Otherwise the UNLOAD data set cannot be properly loaded to the relational database and enhanced compliance reporting capabilities are not available.

   For more information see the JCL Requirements and Control Statements topics for each product in the CA ACF2 or CA Top Secret *Compliance Information Analysis Guide*.

Load the CIA Repository

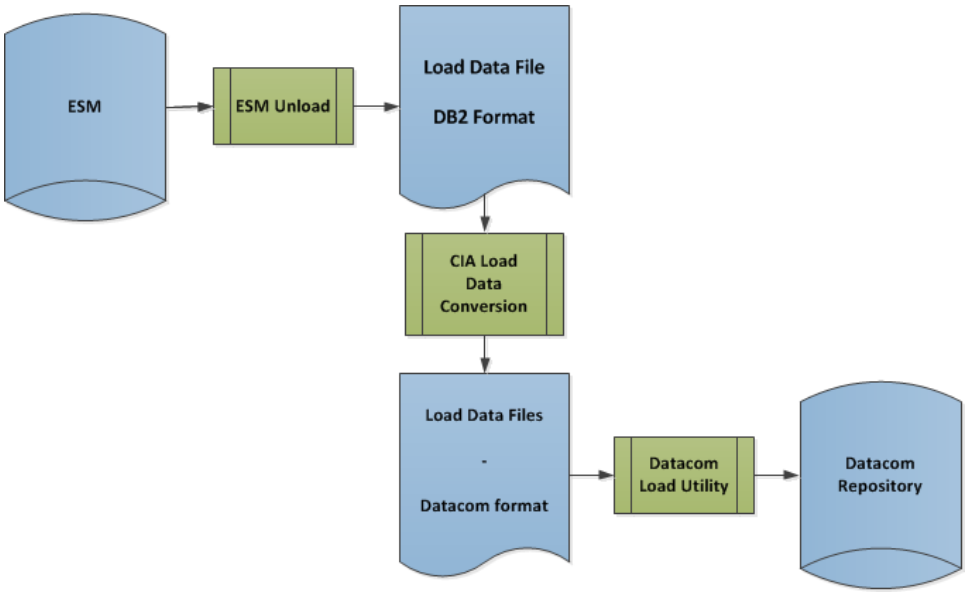
After the CIA repository has been defined to CA Datacom/AD or DB2 and the security information has been unloaded to the UNLOAD data set, the security information can be loaded into the CIA repository. The CA Datacom/AD DBUTLTY program or the IBM DB2 LOAD utility is used to insert the security information into the CIA repository.

The Load Process for CA Datacom/AD

The CIAUNLD job executes the unload utility, which reads the security information from the security database and creates an unload data set.

The unload data set is used as input to the CIALOADC job. Since the unload data set is in DB2 load format, the CIALOADC job converts the user and security policy information in the unload data set from DB2 load format to CA Datacom/AD load format and separates the converted records into individual data sets by table as required by the CA Datacom/AD load process.

The following illustrates the unload/load process for CA Datacom/AD.



Estimate the Storage Requirements for CA Datacom/AD Load Format Data Sets

Estimate the amount of space that is required for each CA Datacom/AD load format data set populated by the conversion utility. Since these data sets can contain large amounts of security data, allocate each data set with enough space to allow conversion utility processing to complete successfully.

Follow these steps:

1. After running the CIAUNLD CIA unload utility, review the output Statistical Report to find the number of records generated for each of the CIA tables.
2. For each CIA table, multiply the number of records generated for the CIA table by the maximum CIA table record length (3,157 bytes) to determine the maximum number of bytes of storage required for each CIA output data set.
3. Divide the total number of bytes of storage required by the number of bytes on a cylinder for the hardware disk model you are using

Use the following equation to estimate the amount of space that is needed for each output data set:

The maximum count of a CIA table record type generated x [maximum CIA table record length (3,157 bytes) / 849,960 bytes = _____ Total space (in cylinders)

You have determined the total number of cylinders of space to allocate for each CA Datacom/AD load format data set.

Load the Security Information into a CA Datacom/AD Repository

After the CIA application and repository is defined to CA Datacom/AD and the security information is unloaded with the CIAUNLD job, the CIALOADC job converts the unloaded security information from DB2 load format into CA Datacom/AD load format and separates the converted records into individual data sets by table as required by the CA Datacom/AD load process. It then executes the CA Datacom/AD DBUTLTY program to load the security information into the CIA repository tables.

The CIALOADC job consists of the following steps:

- DELETE. Deletes existing CA Datacom/AD load format data sets.
- CONVERT. Executes the CIADCCNV conversion utility to convert the unload data set created by the CIAUNLD job into the appropriate CA Datacom/AD load format data sets.
- CLEARDB. Deletes any information currently in the CIA repository tables.
- LOAD. Executes the CA Datacom/AD DBUTLTY program to load the security information into the CIA repository tables.

  Note: The CLEARDB step of this job deletes all existing data in the current CIA repository tables. If you wish to add new data to an existing CIA repository, remove the CLEARDB step from the job before execution.

Follow these steps:

1. Edit the CIALOADC job in one of the following libraries:
   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and Customization sections of the job to customize the job for your environment.

2. Adjust the space allocations within the CONVERT step based on the storage requirements estimated for each of the CA Datacom/AD UNLOAD data sets . For more information, see Estimate the Storage Requirements for CA Datacom/AD Load Format Data Sets.
3. The CLEARDB step of this job deletes all existing data in the current CIA repository tables. If you are adding new data to an existing CIA repository, remove the CLEARDB step from the job before execution
4. Submit the job.

   The job executes and completes
5. Verify the output of the CIALOADC.

   Check the output of the CIALOADC job, verifying that the security information has been loaded successfully.

   Note: The CIA load data conversion utility executed by the CONVERT step returns the following codes:

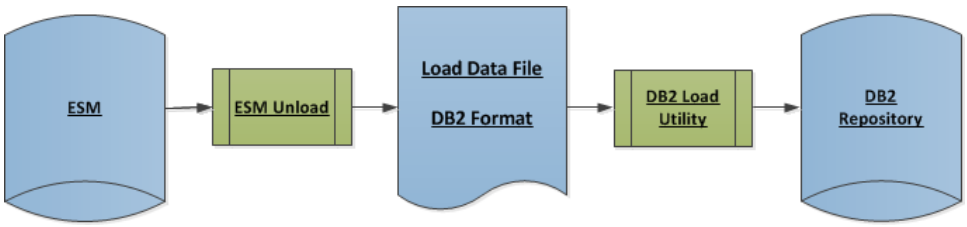
   - 0 - Data conversion process was successful.
   - 12 - Data conversion process failed. A diagnostic message was issued.

Note: Each time you run the Unload utility, run the conversion utility to replicate the most current information in the CIA repository.

The Load Process for DB2

The CIAUNLD job executes the unload utility, which reads the security information from the security database and creates an unload data set. This unload data set is used as input to the DB2 load process which loads the data into a DB2 repository.

The following illustrates the unload/load process for DB2.



Load the Security Information into DB2

After the DB2 repository has been defined to DB2 and the security information has been unloaded to the UNLOAD data set, the security information can be loaded into the DB2 repository. The IBM DB2 LOAD utility is used to insert the security information into the DB2 database.

The CIALOAD job executes a series of steps to load security information into the repository in the target DB2 subsystem.

Important! This job replaces all existing data in the CIA repository. If you want to load additional data from additional systems after you have loaded one system, use the CIALOADA job for each subsequent load, so the existing CIA data is retained in the Repository.

Follow these steps:

1. Edit the CIALOAD job (or CIALOADA job, if you want to add additional data to the repository) in one of the following libraries:

   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Modify the job to conform to your installation standards directing it to the target DB2 subsystem where the repository is defined. Follow the instructions in the Notes and Customization sections of the job to customize the job for your environment.

   Note: The DB2 LOAD utility requires DFSORT. If DFSORT is not your default sort program, add a STEPLIB to the CIALOAD and CIALOADA jobs to specify the correct libraries where DFSORT resides.

2. Submit the job.

   The job runs and completes.

3. Verify the output of the CIALOAD job (or CIALOADA job).

   The security information is loaded.

Note: Each time you run the Unload utility, run the Load utility to replicate the most current information in the CIA repository.

Allocate the CIA Real-Time Output Data Sets

The CIA real-time status file (CIASTATS DD) is an optional output data set that records the results of STATUS console commands processed by the CIA real-time component. The CIA real-time journal file (CIAJRNL DD) is an optional output data set that records messages about internal warnings and failures that occur during the processing of an update event. The journal data set is a wraparound data set.

The CIARTALC job allocates these output data sets.

Follow these steps:

1. Edit the CIARTALC job in one of the following libraries.
   - CA ACF2 - CAI.CAX1JCL0
   - CA Top Secret - CAI.CAK0JCL0

   Follow the instructions in the job to modify its contents. Estimate the amount of space required for the data sets and modify the space parameters, as necessary.

   Important! Size the data sets correctly at creation so that required entries are not lost.
2. Submit the CIARTALC job.
3. Verify that the CIASTATS DD and CIAJRNL DD data sets were successfully created by checking the job output.

Define the CIA Real-Time Component Procedure

The CIA real-time component is a started task address space that requires a started task procedure.

Follow these steps:

1. Copy the sample CIARTUPD procedure from the CAI.CAX1JCL0 (for CA ACF2) or CAI.CAK0JCL0 (for CA Top Secret) installation data set to a procedure library in each z/OS system where the CIA real-time component is executed.
2. Edit the CIARTUPD procedure in the z/OS system procedure library to conform to your installation standards.
   - If you supply option overrides at component start-up, verify that member CIAPARMS exists and is specified in the CIAPARMS DD statement.
   - If you record the output of the STATUS command to a data set, verify that the CIASTATS DD statement points to an existing status data set.
   - If you record update request failures to a data set, verify that the CIAJRNL DD statement points to an existing journal data set.

The CIA real-time component procedure contains the following JCL statements:

CIARTUPD

Executes the APF-authorized program CIARTINT to start the CIA real-time component.

STEPLIB DD

Specifies the library where the CIA real-time component programs reside. This parameter is optional if the library has been added to the system LINKLIST. If CA Datacom/AD is selected as the repository for the CIA real-time database, you may also have to add a STEPLIB DD for the CAAXLOAD library if it has not been added to the system LINKLIST.

CIAJRNL DD

Specifies an optional output data set (or spooled output file SYSOUT) that records journal entries generated during the processing of update requests within the CIA real-time component. These journal entries contain request information and messages that reflect internal warnings or failures that occur during the processing of an event.

CIASTATS DD

Specifies an optional output data set (or spooled output file SYSOUT) that records the results of STATUS commands processed by the CIA real-time component.

CIAPARMS DD

Specifies an optional input data set member that supplies input control options to the CIA real-time component.

Start the CIA Real-Time Component

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

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

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

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

Automatically Start During Initialization

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

Start with a Console Command

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

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

```
S CIARTUPD
```

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

Stop the CIA Real-Time Component

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

```
P CIARTUPD
```

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

Control and Modify the CIA Real-Time Component

The CIA real-time component includes a console interface that you can use to control the execution of the CIA real-time component address space.

Note: In all of the examples below, CIARTUPD is used as the name of the CIA real-time component started task. If you changed the name of the CIA real-time component procedure, specify that value in the command rather than CIARTUPD.

Issue the following console command:

F CIARTUPD,*xxxxxxxx yyyyyyyy*

CIARTUPD

Specifies the active CIA real-time component procedure.

xxxxxxxx

Specifies the CIA real-time component console command operand.

yyyyyyyy

Specifies optional data for the command operand.

CIA Real-Time Component Command Syntax

The following table lists the CIA real-time component syntax.

Command	Operand	Description
S CIARTUPD	n/a	Starts the CIA real-time component address space
F CIARTUPD	,GTRACE	Activates general trace facility (GTF)
	,NOGTRACE	Deactivates general trace facility (GTF)
	,STATUS	Displays component status to the console and an optional data set
	,RELOAD *module*	Loads a new copy of a module into the component address space
	,RESET *ddname*	Reset the file identified by *ddname*
P CIARTUPD	n/a	Terminates the CIA real-time component address space

Console Command Descriptions

The CIA real-time component supports the following console commands and parameters:

GTRACE

Activates the GTF trace option to write trace entries to the active trace file. This option requires GTF to be active for USRP entries with an ID of X'035'.

Note: We recommend not activating GTF tracing unless instructed to do so by CA Technical Support.

NOGTRACE

Deactivates the GTF option. Trace entries are no longer written to the trace file.

STATUS

Displays a status of current data from the component. The status is written to the console, and to an optional status data set if a DD statement for CIASTATS is included in the component started task procedure JCL.

RELOAD module

Loads a new copy of a CIA real-time component module into the active address space. Specify the name of the module to be loaded as an operand of the RELOAD command.

Note: Use the RELOAD command only under direction of CA Technical Support personnel, or in response to application of CIA real-time component maintenance as documented in the PTF instructions.

RESET ddname

Identifies a file by ddname that resets the next time output is written to the file. The file is opened for OUTPUT in lieu of EXTEND, which causes all data currently in the file erased and output directed to the first block of the file. This command does not affect spooled output.

CIA Real-Time Component Status

The CIA real-time component status provides information about the active component options, logstream statistics, server statistics, and buffer usage. When the STATUS command is issued, the component writes the status information to the console, and to a data set that was configured before the component was started.

Sample CIA Real-Time Component Output

This example shows a sample of the CIA real-time component output resulting from the STATUS command:

```
CIA0440I  *** CIA/RT Component Status ***
CIA0440I    Active ESM    = your ESM
CIA0440I    GTRACE        = Inactive
CIA0440I    Log Stream    = CIA11.SYSLOG
CIA0440I    CIA SYSID     = XE11
CIA0440I    DSI Host Name = 141.202.204.11
CIA0440I    DSI Port #    =  1990
CIA0440I    Timer         =    30 seconds
CIA0440I    Trace size    =   256 K
CIA0440I    Logger Statistics:
CIA0440I       Logger READs        =           18
CIA0440I       Logger DELETEs      =           18
CIA0440I       Logger WAITs        =           16
CIA0440I    Server Statistics:
CIA0440I                     Status      Use Count     Wait Count
CIA0440I       Server   1:  Idle              18             16
CIA0440I    Buffer Statistics:
CIA0440I                       Size      Use Count    Event Count
CIA0440I       Buffer   1:      4K             18             18
```

Active ESM

Specifies the active external security manager (ESM) on this z/OS image.

GTRACE

Specifies the status of the GTRACE option (active or inactive).

Log Stream

Specifies the name of the connected CIA real-time feature logstream.

CIA SYSID

Specifies the name of the SYSID that was used for this security database image when it was loaded into the CIA repository.

DSI Host Name

Specifies the active host name for the CA DSI Server.

DSI Port #

Specifies the active port number for the CA DSI Server.

Timer

Specifies the interval for timed processes in seconds.

Trace Size

Specifies the size of the internal trace table in kilobytes (KB).

Logger READs

Specifies the total number of successful read requests for update records from the CIA real-time feature logstream.

Logger DELETEs

Specifies the total number of successful delete requests for update records in the CIA real-time feature logstream.

Logger WAITs

Specifies the total number of times the communication task waited for a new update request to process.

Server *nnn*

Specifies the current server status:

active

Indicates the number of times the server was used to process request buffers.

idle

Indicates the number of times the server waited to be scheduled for work.

inactive

Displays server statistics line when the server has processed at least one request buffer.

Buffer *nnn*

Reflects the buffer size in kilobytes (KB), the number of times the buffer processed events, and the total count of processed event records. A buffer statistics line displays for each policy buffer that has processed events.

Chapter 8: Implementing CA Compliance Manager for CA Chorus for Security and Compliance Management

CA Compliance Manager and CA Chorus

CA Compliance Manager provides comprehensive compliance management, analysis, and reporting, and is comprised of multiple, discrete components. Some of these components collect and process information about external security manager (ESM) security events. Other components seamlessly monitor your system in real time for changes to critical resources—security records, security configuration options, system data sets, and z/OS configuration controls. In addition, through sophisticated data gathering and data warehousing processes, CA Compliance Manager provides detailed and advanced compliance reporting on all data that it collects.

An instance of CA Compliance Manager exists on each z/OS LPAR that is being monitored. Each instance of CA Compliance Manager has a set of repositories that are defined to CA Datacom/AD or DB2. The repositories contain the information about security events and changes to critical system resources on that LPAR.

CA Chorus for Security and Compliance Management leverages the information from the CA Compliance Manager repositories on each system to provide security event information to the CA Chorus security discipline user.

CA Chorus can access information from multiple instances of CA Compliance Manager. When each instance of CA Compliance Manager is established, CA Chorus can be configured to access the information in that CA Compliance Manager Warehouse or Data Mart repository.

Note: Implementation of CA Compliance Manager is documented in the CA Compliance Manager for z/OS *Implementation Guide*. Use that guide as the principal reference in the implementation of CA Compliance Manager.

Configure CA LDAP Server and CA Compliance Manager

The CDT9PCHR job creates and initializes the CA Compliance Manager policy file.

Important! This procedure was completed during installation of CA LDAP Server. If not, use this procedure to configure CA LDAP Server and CA Compliance Manager.

Follow these steps:

1. Create and initialize the policy file by performing the following substeps:

   Note: The policy file holds the policy statements and policy sets that control component processing for CA Compliance Manager. Create and initialize the policy file before using the CA Compliance Manager and activating its components.

   a. Edit the CDT9PCHR job in *your_ldap_hlq*.CDT9JCL to conform to your site standards, including changing the CA LDAP Server directory names.

   b. Estimate the amount of space required to store the policy statements and policy sets in the policy file and modify the space parameter in CDT9PCHR, as necessary.

   c. Submit the CDT9PCHR job.

      The job runs and completes. This job may take several minutes to complete.

   d. Check the job output to verify that you successfully created the policy file under the name that you specified in the CDT9PCHR job.

      The policy file is ready for use with CA Compliance Manager.

2. Update the slapd.conf file to have the appropriate policy file and DB2 table names, including suffix (company name and country code), DB location, DB user, and DB password. If using a Passticket to connect to DB2, omit the DB password and instead specify the DB2 application ID.

   Important! Failure to configure dblocation with the same value as the DDF may result in an authorization error. Failure to configure dbptktapplid with the same value as the LINKNAME value from the DB2 LUNAME results in a Passticket verification error.

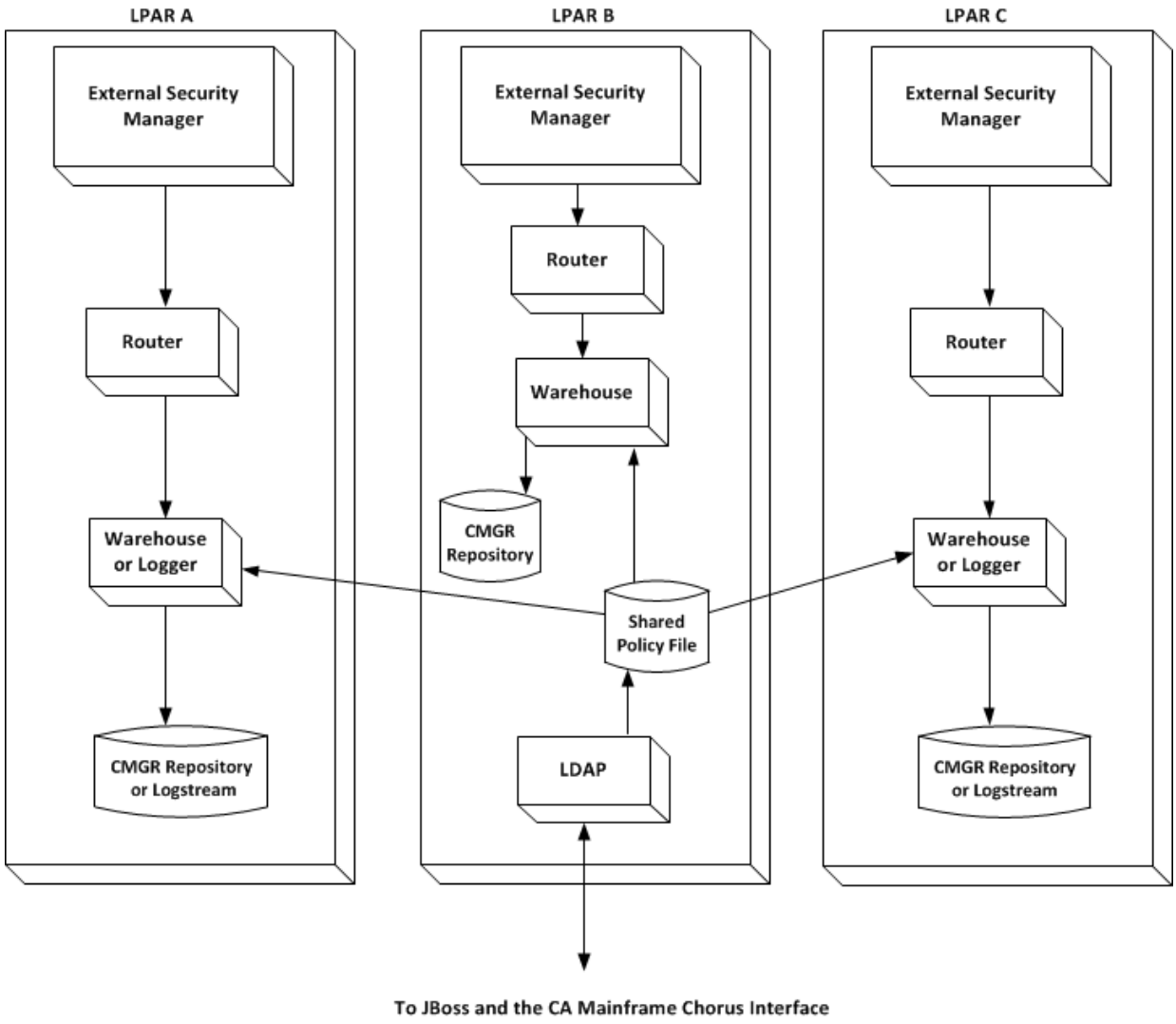
   The slapd.conf file now includes the appropriate policy file and DB2 table names.

3. After you create the policy file and complete the CA Compliance Manager installation and the CA Chorus and CA Chorus for Security and Compliance Management discipline installation, you can use the Administer Compliance Policy quick link in CA Chorus for Security and Compliance Management to define component policy statements and policy sets. We recommend that you regularly back up the policy file by dumping its contents into a data set that you can use later, if necessary, to restore the contents of the current policy file. For backup and restore, use the CDT9PBAC and CDTPRES jobs in *your_ldap_hlq*.CDT9JCL.

   Note: Default policies for each of the CA Compliance Manager components are automatically installed when the policy file is created and initialized.

Sample Configuration for Policy Administration

The following diagram shows a sample configuration for enterprise policy administration:



This diagram shows a sample configuration for enterprise policy administration with the CA Chorus UI and policy database running on LPAR B. The following processing occurs:

- The CA LDAP Server on LPAR B performs policy administration against the shared policy database that it provides to the UI. The policy database contains the tables CA LDAP Server queries when summary reports are run through the Policy Administration UI. The shared policy database communicates with the Router and Warehouse components to obtain data from your external security manager. CA LDAP Server performs policy administration against the policy file.
- LPAR A and C provide data to the shared policy database through your external security manager, router, and warehouse or logger. The data is also provided to the CA Compliance Manager repository or the log stream.

Implement CA Compliance Manager CA Datacom/AD Repositories

If you implement the CA Compliance Manager repositories in CA Datacom/AD, execute the following steps:

- Create the CA Datacom/AD MUF
- Start the CA Datacom/AD MUF
- Delete CA Compliance Manager CA Datacom/AD repositories (if required)
- Define the CA Compliance Manager CA Datacom/AD repositories
- Implement CA Datacom/AD Server

Create the CA Datacom/AD MUF for CA Compliance Manager

Create and deploy a new and empty CA Datacom/AD MUF that holds the CA Compliance Manager repositories you are implementing. For more information, see the CA Datacom/AD *Installation Guide*.

Follow these steps:

1. Edit and submit the CA Datacom/AD AXCUS00 job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job builds, populates, and mass-edits the installation JCL data set.

2. Edit and submit the CA Datacom/AD AXCUS01 job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job Includes all customization for the CA Datacom/AD MUF for CA Compliance Manager.

3. Edit and submit the CA Datacom/AD AXNEW01 job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job allocates and populates data sets that the CA Datacom/AD MUF for CA Compliance Manager needs.

4. Edit and submit the AXRIM01 job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job Installs the PC CALLS.

5. Edit and submit the AXAPFADD job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job provides a CA SYSVIEW example to dynamically add libraries to be APF listed.

6. Edit and submit the AD14STRT job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This job is the procedure that starts the CA Datacom/AD MUF for CA Compliance Manager (CMGRMUF).

   The AD14STRT job can also be used to create the MUF as a started task procedure. For more information, see Create the CA Datacom/AD MUF for CA Compliance Manager as a Started Task Procedure (see page 140).

7. Edit and submit the AXIVP01 job.

   Follow the instructions in the job for modifying it. Verify that the job ran successfully.

   Note: This is a sample install verification job.

8. Edit and submit the AD14STOP job.

   Follow the instructions in the job for modifying. Verify that the job ran successfully.

9. After creating and deploying the CA Datacom/AD MUF, copy the CMGRMUF sample procedure from CAI.CEIQPROC procedure library in the z/OS system where the CIA real-time component is executed.

10. Edit the CMGRMUF procedure to conform to your installation standards.

Note: The CMGRMUF procedure references CA Datacom/AD initialization parameters that are distributed in the CAI.CEIQOPTN installation data set. These parameters can be copied to a parameter data set for the execution JCL. Do not change the values for these initialization parameters unless requested to do so by CA technical support.

Create the CA Datacom/AD MUF for CA Compliance Manager as a Started Task Procedure

Use the following procedure to create the CA Datacom/AD MUF for CA Compliance Manager as a started task procedure.

Follow these steps:

1. Follow the documented CA Datacom/AD rules on how to modify a JCL job to create the MUF as a started task procedure.
2. Copy the AD14STRT job from *your_datacom_hlq*.INSTJCL into the z/OS system procedure library from which CA Compliance Manager components are executed.
3. Rename the AD14STRT job as the CA Datacom/AD MUF that you recorded in your Site Preparation Worksheet. For example, CMGRMUF.
4. The installed CA Datacom/AD MUF must use the settings from AXDATIN1 and AXDATIN2, which contain initialization parameters, and reside in the following CAI.CEIQOPTN library.

   Important! DO NOT change the values for these initialization parameters unless requested to do so by CA technical support.
5. Copy the AXDATIN1 and AXDATIN2 members from the installation data set to a library you choose.
6. Modify the CA Datacom/AD MUF started task procedure to reference the location of the AXDATIN1 and AXDATIN2 members.

Start the CA Datacom/AD MUF for CA Compliance Manager

The CA Datacom/AD MUF must be executing before the CA Compliance Manager repositories can be defined.

Follow these steps:

1. Start the CMGRMUF by issuing the following console command.

   ```
   S CMGRMUF
   ```

   Note: If you created a MUF with a name that is different than the recommended default, CMGRMUF, use the correct MUF name in the command.
2. Verify that the CMGRMUF successfully started.

   Note: For complete information about executing the CA Datacom/AD MUF, see the CA Datacom/AD *Installation Guide for z/OS*.

Delete the CA Compliance Manager Repositories (If Required)

Important! Do not delete, redefine, or reload any of your existing repositories unless you are changing your implementation of CA Compliance Manager. For more information about migrating CA Compliance Manager from CA Chorus r2.5 or r3 to v4.0, see Migrating CA Chorus for Security and Compliance Management to CA Chorus v4.0.

Existing CA Compliance Manager CA Datacom/AD repositories must be deleted so that they can be redefined. The CMGRIDCD job deletes existing repositories.

Follow these steps:

1. Edit the CMGRIDCD job in CAI.CEIQJCL0.

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and the Customization sections of the job to customize the job for your environment.

2. Submit the job.

   The job runs and completes.

3. Verify the output of the CMGRIDCD job.

   The existing CA Compliance Manager repositories are successfully deleted.

Define CA Compliance Manager Repositories for CA Datacom/AD

The CMGRIDCM job performs the tasks of defining the database, tables, and applications in a CA Datacom/AD environment for the following CA Compliance Manager components.

- Warehouse
- Data Mart
- Monitor

Follow these steps:

1. Edit the CMGRIDCM job in CAI.CEIQJCL0.

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and Customization sections of the job to customize the job for your environment.

   Note: The CMGRIDCM job contains multiple steps that define the CA Datacom/AD repositories for the Warehouse, Data Mart, and Monitor components.

   Important! Delete the job steps that define the repository for the CA Compliance Manager components that you are not running.

2. Submit the CMGRIDCM job.
3. Review the output of the CMGRIDCM job to verify that the repositories are successfully defined.

Implement CA Datacom/AD Server for CA Compliance Manager

If you are implementing a CA Datacom/AD repository for CA Compliance Manager, configuration of the CA Datacom/AD Server is required for the following reasons:

- To enable PassTicket authentication (see PassTicket Configuration to Connect to CA Datacom/AD in this guide)
- To provide a gateway from the JDBC and ODBC drivers to the CA Datacom/AD CA Compliance Manager MUF
- To allow CA Datacom/AD Server to access the CA Compliance Manager repositories in the CA Datacom/AD MUF for CA Compliance Manager

Important! The CA Datacom/AD Server must be implemented on the same LPAR as the CA Datacom/AD MUF containing the CA Compliance Manager repositories.

Create the CA Datacom/AD Server Procedure for CA Compliance Manager

After creating and deploying the CA Datacom/AD Server, use the following procedure to create the CA Datacom/AD Server started task procedure.

Follow these steps:

1. Follow the documented CA Datacom/AD rules on how to modify a job to create it as a started task procedure.
2. Copy the sample JCL job from the CA Datacom/AD Server installation data set to the library from which it will be executed as a started task procedure and name the procedure appropriately. For example, CMGRSRV.
3. Edit the sample JCL job to create the new started task procedure (CMGRSRV). Conform the procedure to your installation standards and to match the values in the CA Datacom/AD installation data sets that were used to create the CA Datacom/AD MUF for CA Compliance Manager.
4. Add the your_chorus_hlq.CETJPLD target library from the CA Chorus platform installation to the STEPLIB concatenation in the procedure.
5. Verify that all libraries that are in the STEPLIB concatenation of the procedure are APF-authorized.

Configure CA Datacom/AD Server to Connect to CA Datacom/AD for CA Compliance Manager

After deploying the CA Datacom/AD Server, perform the following procedure to configure the CA Datacom/AD Server to connect to the MUF for CA Compliance Manager

The CA Datacom/AD Server parameters for CA Compliance Manager are located in the CMGRSRVP and HEAPCHK members in the following CAI.CEIQOPTN.

Note: For more information about implementing the CA Datacom/AD Server, see the CA Datacom/AD Server *User Guide*.

Follow these steps:

1. Copy the CMGRSRVP and HEAPCK members to a library you choose.
2. Modify the CA Datacom/AD Server started task procedure (for example, CMGRSRV) to reference the location of the CMGRSRVP and HEAPCK members.
3. If you are using a separate MUF for the CA Compliance Manager repositories than the one for CIA (recommended), ensure that the initialization parameters for the CA Datacom/AD Server for CA Compliance Manager have the following values:

```
SERVERNAME=CMGRx_SYSy
APPLID=CMGRx_SYSy
PLANNAME=$MBH
AUTHID=SYSUSR
PROTOCOL=BOTH
TCPIP_HOST=LPARNAME
DBUSERS=900
TIMEOUT=6
TIMEOUTWAIT=10
LOGON=YES
CHORUSEXT=CHRCXT10
```

4. If you are using the same MUF for the CA Compliance Manager repositories and the CIA repository (sharing a MUF), ensure that the initialization parameters for the CA Datacom/AD Server for CA Compliance Manager have the following values:

   Important! The CA Datacom/AD Server initialization parameter values for CA Compliance Manager must be the same as the CA Datacom/AD Server initialization parameter values for CIA.

   ```
   SERVERNAME=CMGRx_SYSy
   APPLID=CMGRx_SYSy
   PLANNAME=$MBH
   AUTHID=SYSUSR
   PROTOCOL=BOTH
   TCPIP_HOST=LPARNAME
   DBUSERS=900
   TIMEOUT=6
   TIMEOUTWAIT=10
   LOGON=YES
   CHORUSEXT=CHRCXT10
   ```

Start CA Datacom/AD Server for the CA Datacom/AD MUF for CA Compliance Manager

After the CA Datacom/AD MUF has been started, and the CA Datacom/AD Server has been configured, CA Datacom/AD Server must be started for the CA Datacom/AD MUF for CA Compliance Manager.

Follow these steps:

1. Start the CA Datacom/AD Server by issuing a console command to execute the started task procedure. For example:

   ```
   'S CMGRSRV'
   ```

   Note: If you created the CA Datacom/AD Server started task procedure with a name that is different than the recommended default, CMGRSRV, use the correct started task procedure name in the command.

2. Verify that the CA Datacom/AD Server was successfully started.

Note: For more information about starting CA Datacom/AD Server, see CA Datacom/AD Server *User Guide*.

Migrating from DB2 to CA Datacom/AD Repositories

If migration from DB2 to CA Datacom/AD is required, see the CA Compliance Manager *Implementation Guide* for more information.

Implement the CA Compliance Manager DB2 Repositories

If you implement CA Compliance Manager repositories in DB2, the following steps are required:

- Set up Workload Manager (WLM) and Resource Recovery Attach Facility (RRSAF)
- Create the DB2 subsystem
- Start the DB2 subsystem
- Define the CIA repository for DB2

Set Up Workload Manager (WLM) and Resource Recovery Attach Facility (RRSAF)

The CA Compliance Manager Warehouse and Monitor components use RRSAF to connect to and communicate with DB2 to process SQL statements. Before you activate the Warehouse or Monitor components, RRSAF must be active.

Follow these steps:

1. Verify that Resource Recovery Services Attachment Facility (RRSAF) is set up.
2. If you have not set up your DB2 environment to use WLM-established address spaces, see the *IBM Redbook, DB2 for z/OS Stored Procedures: Through the CALL and Beyond* for directions on setting up WLM and RRSAF for this purpose.

   Note: We recommend that you set up a separate WLM environment for the CIA user-defined functions and stored procedure.
3. Start RRASF on the z/OS system by issuing a console command that executes the procedure. For example:

   ```
   S RRS
   ```

Create the DB2 Subsystem

For complete information about creating and deploying a DB2 subsystem, see the appropriate IBM DB2 documentation.

Follow these steps:

1. Verify the name of the DB2 subsystem you are using to hold the CA Compliance Manager repositories.
2. Create and deploy the DB2 subsystem that holds the CA Compliance Manager repositories.

Start the DB2 Subsystem

The DB2 subsystem must be executing before the CA Compliance Manager repositories can be defined.

Follow these steps:

1. Verify that RRASF is running, before starting the DB2 subsystem.
2. Start the DB2 subsystem by issuing a console command that executes the procedure. For example:

   ```
   +DSNCSTART DB2
   ```

3. Verify that the DB2 subsystem successfully started.

Note: For complete information about executing the DB2 subsystem, see the appropriate IBM DB2 documentation.

Define the CA Compliance Manager Repositories for DB2

The CMGRIDB2 job defines the DB2 repositories for the following CA Compliance Manager components:

- Warehouse
- Data Mart
- Monitor

Follow these steps:

1. Edit the CMGRIDB2 job in CAI.CEIQJCL0.

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and the Customization sections of the job to customize the job for your environment.

   Note: The CMGRIDB2 job contains multiple steps. The job defines the DB2 repositories for the Warehouse, Data Mart, and Monitor components. The CMGRIDB2 job binds the CA Compliance Manager plans, and using native DB2 security, grants access to DB2 resources to the component started tasks.
2. Delete the job steps that define the repository for the CA Compliance Manager components that you are not running.
3. Submit the CMGRIDB2 job.
4. Review the output of the CMGRIDB2 job.

   Verify that the repositories are successfully defined, the plans are bound, and the GRANT statements are successful.

Allocate the CA Compliance Manager Component Output Data Sets

The CMGRIALC job allocates the optional status and journal output data sets for the following CA Compliance Manager components:

- Router
- Alert
- Logger
- Warehouse
- Monitor

The status file (CMGRSTAT DD) is an optional output data set that records the results of STATUS console commands processed by the CA Compliance Manager components.

The journal file (CMGRJRNL DD) is an optional output data set that records the completion status of alerts that were generated by the Alert and Monitor components.

Follow these steps:

1. Edit the CMGRIALC job in CAI.CEIQJCL0.

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and the Customization sections of the job to customize the job for your environment. Estimate the amount of space that is required and modify the space parameters, as necessary.

   Important! Size the data sets correctly at creation so that required entries are not lost.

2. Submit the CMGRIALC job.
3. Review the output of the CMGRIALC job.

   Verify that the data sets were created.

Determine Which Type of z/OS System Logstream to Define

Determine which type of System Logger logstream to define for use by the CA Compliance Manager Logger component and Data Mart. You can use a DASD-only or Coupling Facility (CF)-based logstream.

A DASD only based logstream stores security event data in local storage buffers and a DASD-based staging data set. A CF-based logstream stores the security event data in a Coupling Facility List structure.

Note: For more information about defining and maintaining a z/OS system Coupling Facility (CF) or DASD-only logstream, see IBM documentation.

Define a DASD-Only Logstream

The CMGRLDEF job defines a DASD-only system logstream using the IBM Utility, IXCMIAPU.

Follow these steps:

1. Edit the CMGRLDEF job in CAI.CEIQJCL0.
2. Delete STEP2 and STEP3.

   Note: STEP2 and STEP3 are used only for defining a CF-based system logstream.
3. Edit STEP1.

   Modify the job statements to conform to your installation standards.
4. Submit the job.
5. Review the output of the CMGRLDEF job.

   Verify that the job completed successfully, and that the system logstream was defined.

Define a CF-Based Logstream

The CMGRLDEF job defines a Coupling Facility (CF)-based system logstream using the IBM Utility, IXCMIAPU.

Follow these steps:

1. Edit the CMGRLDEF job in CAI.CEIQJCL0.
2. Delete STEP1.

   Note: STEP1 is used only for defining a DASD-only logstream.
3. Edit STEP2

   Modify the job statements to conform to your installation standards.
4. Edit STEP3

   Modify the job statements to conform to your installation standards.

   Note: This STEP merges the CFRM structure definition into the current active CFRM policy (in STEP2).
5. Submit the job.
6. Review the output of the CMGRLDEF job.

   Verify that the job completed successfully, and that the CF-based logstream was defined.

Enable SSL for CA Compliance Manager Chorus Alerts

This procedure enables the CA Compliance Manager Alert and Monitor components to send CA Chorus Alerts using SSL.

Note: Do this procedure for *both* the Alert and Monitor started tasks.

Follow these steps:

1. Review the Monitor and Alert started tasks procedures for a CEEOPTS DD. If a CEEOPTS DD already exists, skip this step and proceed to step 2.

   If a CEEOPTS DD does not exist, add one.

   Example:

   ```
   //CEEOPTS DD DISP=SHR,DSN=your.proclib(CMGROPTS)
   ```

   Note: 'CMGROPTS' is an example of a PDS member name. Use any member name as long as it meets the standard PDS naming conventions.

2. Edit the 'CMGROPTS' PDS member referenced by the CEEOPTS DD so that it has the following configuration parameters:

   ```
   TRAP(OFF),POSIX(ON)
   ENVAR("_CEE_ENVFILE_S=DD:STDENV")
   ```

3. In the Monitor and Alert started task procedures, add a STDENV DD.

   Example:

   ```
   //STDENV DD DISP=SHR,DSN=your.proclib(ALERTS)
   ```

   Note: 'ALERTS' is an example of a PDS member name. Use any member name as long as it meets the standard PDS naming conventions.

4. If you are using a key database, skip this step and proceed to step 5.

   If you are using a keyring, create the 'ALERTS' PDS member referenced by the STDENV DD so that it has the following configuration parameters:

   ```
   AXIS2C_CERT_KEYFILE=userid/ringname
   ```

   Replace the ‘userid/ringname’ text with the name of the key ring.

   Important! The user ID of the started task must be permitted access to the IRR.DIGTCERT.LISTRING resource in the FACILITIES task. If the user ID specified in the environment file above is the same as the user ID of the started task, then you must permit READ access; otherwise, if the user IDs are not the same, you must grant UPDATE access.

   Important! The key ring name is *case sensitive*. Enter the exact name of the key ring.

   The name of the key ring can be obtained through the security package as follows:

   - For CA ACF2, enter the following commands:

```
set prof(user) div(keyring)
list like(startedtask_logonid-)
```

startedtask_logonid

Specifies the logonid associated with the CA Compliance Manager alerts started task.

- For CA Top Secret, enter the following commands:

```
tss list(startedtask_logonid) segment(keyring)
```

startedtask_logonid

Specifies the logonid associated with the CA Compliance Manager alerts started task.

After making these changes, but before starting the alert component, create the key ring and connect the appropriate certificate to it. The appropriate certificate is the root CA certificate that signed the certificate that the CA Chorus Application Server uses. You can use the Java keytool utility to export this certificate from the key store of the CA Chorus Application Server server. Import the certificate into the security manager on the system that will run the alert component and connect it to the alert component's key ring. The certificate should be associated with either the user ID of the alert component or to the CERTAUTH ID. If you do not associate the certificate with the CERTAUTH ID, you must specify "USAGE(CERTAUTH)" when connecting the certificate to the key ring.

5. *If you are using a key database*, create the 'ALERTS' PDS member referenced by the STDENV DD so that it has the following configuration parameters:

```
AXIS2C_CERT_KEYFILE=/dir/dbname
AXIS2C_CERT_LABEL=label
AXIS2C_CERT_PASSWRD=passwrd
```

- Replace '/dir/dbname' with the fully qualified name of the key database file.
- Replace 'label' with the label of the certificate in the key database that will be used to connect to the CA Chorus Application Server.
- Replace 'passwrd' with the password to be used for access to the key database.

Start the CA Compliance Manager Components (Manually)

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

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

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

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

Follow these steps:

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

   ```
   S CMGRRTR
   ```

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

   ```
   S CMGRLOGR
   ```

6. Verify that the Logger component successfully started.

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

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

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

   ```
   F CMGRLOGR,STATUS
   ```

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

   ```
   S CMGRWHSE
   ```

8. Verify that the Warehouse component successfully started.

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

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

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

   ```
   F CMGRWHSE,STATUS
   ```

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

   ```
   S CMGRMON
   ```

10. Verify that the Monitor component successfully started.

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

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

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

    ```
    F CMGRMON,STATUS
    ```

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

    ```
    S CMGRALRT
    ```

12. Verify that the Alert component successfully started.

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

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

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

    ```
    F CMGRALRT,STATUS
    ```

Start the CA Compliance Manager Components (Automatically)

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

Follow these steps:

1. Copy all the CA Compliance Manager started task procedures from the CAI.CEIQPROC library into the library from which the procedures will be executed (for example, SYS1.PROCLIB).

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

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

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

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

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

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

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

Implement the Data Mart

The Data Mart Selection Utility (Data Mart) unloads to a sequential data set a subset of historical security event information from the system logstream, which the Logger component populated in real time. The data must then be loaded into the CA Datacom/AD or DB2 Data Mart Repository that was defined in an earlier step.

Important! The Logger component must have been active for a period of time to record security event information to the system logstream.

If you implement the Data Mart, the following steps are required:

- Define Data Mart Security Event Selection
- Estimate the Space Requirements for the Data Mart Output Data Sets
- Allocate the Data Mart Output Data Sets
- Unload Data from the Logstream Using the Data Mart
- Load the CA Datacom/AD Data Mart Repository
- Load the DB2 Data Mart Repository
- Load Additional Data into an Existing DB2 Data Mart Repository

Define Data Mart Security Event Selection

Data Mart SYSIN DD file input control statements determine the events that the Data Mart unloads from the system logstream. You specify selection criteria in either the Data Mart event policy or the SYSIN DD file input control statements. The more criteria you specify, the more selective the Data Mart is in unloading event information from the logstream. This controlled event selection lets you customize the security event data at any level to meet your installation's unique compliance needs.

Important! Choose only one option for each run of the Data Mart, because these options are mutually exclusive. If you choose more than one option, the Data Mart terminates with an error.

- Option A: Use Data Mart security event policy for event selection.
- Option B: Use SYSIN DD file input control statements for event selection.

Data Mart Security Event Policy for Event Selection (Option A)

Define Data Mart event policy in the event policy database. This policy indicates the security events that are extracted from the system logstream by the Data Mart and loaded into the Data Mart repository.

In addition to defining the Data Mart event policy set, the following are required SYSIN DD input control statements. These statements select each security event record from the logstream that matches the Data Mart event policy:

- POLICYSET(policyset)
- LOGSTREAM(logstream)
- SDATE(mm/dd/yyyy|TODAY|TODAY-nnnn)
- EDATE(mm/dd/yyyy|TODAY|TODAY-nnnn)

Example of Using Data Mart Security Event Policy for Event Selection (Option A)

The following is an example of how to specify Data Mart SYSIN DD input control statements to use a Data Mart policy set named, 'DATAMARTPOLICY1'. This policy set causes the Data Mart to select and process event records from a system logstream named 'CMGR.CF.LGSTRM' that occur between 01/01/2009-00:00:00:01 and 12/31/2009-23:59:59:99 and that match the selection criteria in the policy set.

```
//SYSIN         DD  *
LOGSTREAM(CMGR.CF.LGSTRM)
POLICYSET(DATAMARTPOLICY1)
SDATE(01/01/2009)
STIME(00:00:00:01)
EDATE(12/31/2009)
ETIME(23:59:59:99)
/*
//
```

SYSIN DD Input Control Statements for Event Selection (Option B)

Data Mart SYSIN DD input control statements support general security event selection. You can select events based on start date, start time, end date, end time, system ID, or sysplex name (not both), event name, and user ID. Specifying one or more of the following optional statements causes the Data Mart to select each record from the logstream that matches the value specified in each input control statement:

- LOGSTREAM(*logstream*)
- SDATE(*mm/dd/yyyy*|TODAY|TODAY-*nnnn*)
- EDATE(*mm/dd/yyyy*|TODAY|TODAY-*nnnn*)
- STIME(*hh*|*hh:mm*|*hh:mm:ss*|*hh:mm:ss:th*|00:00:00:01)
- ETIME(*hh*|*hh:mm*|*hh:mm:ss*|*hh:mm:ss:th*|23:59:59:99)
- SYSID(*sysid*)
- SYSPLEX(*sysplex*)

- EVENT(*event*)
- USERID(*userid*)

Note: For this option, LOGSTREAM, SDATE, and EDATE are required.

Example of Using SYSIN DD Input Control Statements for Event Selection (Option B)

The following is an example of how to specify event selection criteria in SYSIN DD input control statements to unload 'SIGNON' and 'SIGNOFF' security events from a system logstream named, 'CMGR.CF.LGSTRM' on system, 'SYS1', that occur between 01/01/2009-00:00:00:01 and 12/31/2009-23:59:59:99 and that have a userid field value that matches 'USER01':

```
//SYSIN         DD  *
LOGSTREAM(CMGR.CF.LGSTRM)
SDATE(01/01/2009)
STIME(00:00:00:01)
EDATE(12/31/2009)
ETIME(23:59:59:99)
SYSID(SYS1)
EVENT(SIGNON)
EVENT(SIGNOFF)
USERID(USER01)
/*
//
```

Data Mart Input Control Statements

The Data Mart supports the following SYSIN DD file input control statements, which control Data Mart processing and select events for unload.

Important! Each input control statement must start on a new line in the SYSIN DD file. Any keywords that you specify after the first keyword on a control statement are ignored. You cannot use masking in input control statements. If you do not specify a SYSIN DD file or input control statements, Data Mart processing terminates with an error.

Input Control Statement Syntax

```
LOGSTREAM(logstream)
SDATE(mm/dd/yyyy|TODAY|TODAY-nnnn)
STIME(hh|hh:mm|hh:mm:ss|hh:mm:ss:th|00:00:00:01)
EDATE(mm/dd/yyyy|TODAY|TODAY-nnnn)
ETIME(hh|hh:mm|hh:mm:ss|hh:mm:ss:th|23:59:59:99)
[NEWSYSID(sysid)]
[{POLICYSET(policyset)} |
       {EVENT(START)}
       {EVENT(STOP)}
       {EVENT(STOPVIO)}
       {EVENT(MODIFY)}
       {EVENT(MODIFYVIO)}
       {EVENT(SIGNON)}
       {EVENT(SIGNONVIO)}
       {EVENT(SIGNOFF)}
       {EVENT(OBJECTACCESS)}
       {EVENT(OBJECTAUDIT)}
       {EVENT(OBJECTVIO)}
       {EVENT(ACCOUNTADMIN)}
       {EVENT(ACCOUNTADMINVIO)}
       {EVENT(POLICYADMIN)}
       {EVENT(POLICYADMINVIO)}
       {EVENT(OTHERADMIN)}
       {EVENT(OTHERADMINVIO)}
       {EVENT(INITUSP)}
       {EVENT(DELETEUSP)}
       {EVENT(R_SETUID)}
       {EVENT(R_SETEUID)}
       {EVENT(R_SETGID)}
       {EVENT(R_SETEGID)}
       {EVENT(INITACEE)}
       {EVENT(CK_ACCESS)}
       {EVENT(R_CHOWN)}
       {EVENT(R_CHMOD)}
       {EVENT(R_CHAUDIT)}
       {EVENT(R_AUDIT)}
       {EVENT(R_SETFACL)}
       {SYSID(sysid)}
       {SYSPLEX(sysplex)}
       {USERID(userid)}]
```

Input Control Statement Descriptions

LOGSTREAM(*logstream*)

Specifies the name of the system logstream which contains the security event records that the Logger component extracted. Do not abbreviate this required keyword. Specify only one LOGSTREAM keyword in the SYSIN control statements.

Limits: 1 to 26 characters, uppercase

SDATE(*mm/dd/yyyy*|TODAY|TODAY-*nnnn*)

Specifies a 10-character string used for two purposes:

- The starting date from which all events are searched in the logstream.
- The starting date to determine whether an event record is selected for unload. Specify the date in the format mm/dd/yyy, , where *mm* is the month, *dd* is the day, and *yyyy* is the year. Specify only one SDATE keyword in the SYSIN control statements. Do not abbreviate this required keyword. Do not specify both *mm/dd/yyyy* and TODAY or TODAY-*nnnn* in the SDATE keyword. (Required)

mm/dd/yyyy

Specifies a 10-character date string in the format *mm/dd/yyyy. mm* is the month, *dd* is the day, and *yyyy* is the year.

TODAY

Represents the current date according to the system clock, and is internally translated to a date in the format mm/dd/yyyy. Use this format if you want to run the Data Mart batch jobs automatically at periodic intervals without requiring modification to this parameter. Do not abbreviate this value.

nnnn

Specifies a one- to four-digit number from 1 to 9999, which represents a negative offset. A negative offset is a number of days in the past from TODAY (the current date). The number is internally combined and interpreted with the TODAY value and translated to a date in the format: mm/dd/yyyy. Use this format if you want to automatically run the Data Mart batch jobs at periodic intervals in the past. This does not require modification to this parameter.

Note: If you also specify the POLICYSET keyword, no selection occurs based on this field. This field is still used with the STIME to determine when to start reading event records from the logstream. The starting date (SDATE) and starting time (STIME) are interpreted internally together as one time stamp value when reading events from the logstream and selecting events based on start date and time. These values are read in local time zone format.

STIME(*hh*|*hh:mm*|*hh:mm:ss*|*hh:mm:ss:th*|<u>00:00:00:01</u>)

(Optional) Specifies a string that is used for two purposes:

- The starting time from which all events are searched in the logstream.
- The starting time to determine whether an event record is selected for unload.

If you specify a string of only *hh* or *hh:mm* or *hh:mm:ss*, by default, the minutes, seconds, tenths, and hundredths of seconds appear as zeros. Specify only one STIME keyword in the SYSIN control statements. Do not abbreviate this optional keyword.

Limits: 2, 5, 8, or 11 characters in the format *hh:mm:ss:th*, where *hh* is hours, *mm* is minutes, *ss* is seconds, and *th* is tenths and hundredths of a second.

Default: 00:00:00:01

Note: If you also specify the POLICYSET keyword, no selection occurs based on this field. This field is still used to determine when to start reading event records from the logstream.

The starting date (SDATE) and starting time (STIME) are interpreted internally together as one time stamp value when reading and selecting events from the logstream. This value is interpreted in local time zone format. For the purposes of internally determining when to start reading event records from the logstream, a time interval of 5 minutes is automatically subtracted from the SDATE/STIME time stamp to help ensure that all requested event records are found in the logstream.

Examples

This example represents the time - 12 hours, 1 minute, 1 second, 100th of a second:

```
STIME(12:01:01:01)
```

This example represents the time - 12 hours, 1 minute, 1 second, 0 hundredths of a second:

```
STIME(12:01:01)
```

This example represents the time - 12 hours, 1 minute, 0 seconds, 0 hundredths of a second:

```
STIME(12:01)
```

This example represents the time - 12 hours, 0 minutes, 0 seconds, 0 hundredths of a second:

```
STIME(12)
```

EDATE(*mm/dd/yyyy*|TODAY|TODAY-*nnnn*)

Specifies a 10-character string used for two purposes:

- The ending date from which all events are searched in the logstream.
- The ending date to determine whether an event record is selected for unload.

Specify the date in the format mm/dd/yyyy, where *mm* is the month, *dd* is the day, and *yyyy* is the year. Specify only one EDATE keyword in the SYSIN control statements. Do not abbreviate this required keyword. Do not specify both *mm/dd/yyyy* and TODAY or TODAY-*nnnn* in the SDATE keyword. (Required)

mm/dd/yyyy

Specifies a 10-character date string in the format *mm/dd/yyyy*, where *mm* is the month, *dd* is the day, and *yyyy* is the year

TODAY

Represents the current date according to the system clock, and is internally translated to a date in the format mm/dd/yyyy. Use this format if you want to automatically run the Data Mart batch jobs at periodic intervals without requiring modification to this parameter. Do not abbreviate this value.

nnnn

Specifies a one- to four-digit number from 1 to 9999, which represents a negative offset—a number of days in the past from TODAY (the current date). The number is internally combined and interpreted with the TODAY value and translated to a date in the format: mm/dd/yyyy. Use this format if you want to automatically run the Data Mart batch jobs at periodic intervals in the past without requiring modification to this parameter.

Note: If you also specify the POLICYSET keyword, no selection occurs based on this field. This field is still used to determine when to stop reading event records from the logstream.

The ending date (EDATE) and ending time (ETIME) are interpreted internally together as one time stamp value for the purposes of reading and selecting events from the logstream. This value is interpreted in local time zone format. For the purposes of internally determining when to stop reading event records from the logstream, a time interval of 5 minutes is automatically added to the EDATE/ETIME time stamp to verify that all event records are found in the logstream.

ETIME(*hh*|*hh:mm*|*hh:mm:ss*|*hh:mm:ss:th*|23:59:59:99)

(Optional) Specifies a string that is used for two purposes:

- The ending time from which all events are searched in the logstream.
- The ending time to determine whether an event record is selected for unload.

If you specify a string of only *hh* or *hh:mm* or *hh:mm:ss*, by default, the minutes, seconds, tenths, and hundredths of seconds each appear as zeros. Specify only one ETIME keyword in the SYSIN control statements. Do not abbreviate this optional keyword.

Limits: 2, 5, 8 or 11 characters in the format *hh:mm:ss:th*, where *hh* is hours, *mm* is minutes, *ss* is seconds, and *th* is tenths and hundredths of a second

Default: 23:59:59:99

Note: If you also specify the POLICYSET keyword, no selection occurs based on this field, although it is still used to determine when to stop reading event records from the logstream.

The ending date (EDATE) and ending time (ETIME) are interpreted internally together as one time stamp value in local time zone format for the purposes of reading events from the logstream and selecting events based on date and time. For the purposes of internally determining when to stop reading event records from the logstream, a time interval of 5 minutes is automatically added to the EDATE/ETIME time stamp to help ensure that all requested event records are found in the logstream.

Examples

The following example represents the time - 23 hours, 59 minutes, 59 seconds, 99 hundredths of a second:

```
ETIME(23:59:59:99)
```

The following example represents the time - 23 hours, 59 minutes, 59 seconds, 0 hundredths of a second:

```
ETIME(23:59:59)
```

The following example represents the time - 23 hours, 59 minutes, 0 seconds, 0 hundredths of a second:

```
ETIME(23:59)
```

The following example represents the time - 23 hours, 0 minutes, 0 seconds, 0 hundredths of a second:

```
ETIME(23)
```

EVENT(*event*)

(Optional) Specifies that logstream event records are selected for unload based on the 1- to 32-character name of a valid CA Compliance Manager security event. Do not abbreviate this optional keyword. You can specify more than one EVENT keyword in the SYSIN control statements. If you do not specify EVENT, no selection occurs based on this field.

Note: EVENT and POLICYSET are mutually exclusive.

Options:

- EVENT(START)
- EVENT(STOP)
- EVENT(STOPVIO)
- EVENT(MODIFY)
- EVENT(MODIFYVIO)
- EVENT(SIGNON)
- EVENT(SIGNONVIO)
- EVENT(SIGNOFF)
- EVENT(OBJECTACCESS)
- EVENT(OBJECTAUDIT)
- EVENT(OBJECTVIO)
- EVENT(ACCOUNTADMIN)
- EVENT(ACCOUNTADMINVIO)
- EVENT(POLICYADMIN)
- EVENT(POLICYADMINVIO)
- EVENT(OTHERADMIN)
- EVENT(OTHERADMINVIO)
- EVENT(INITUSP)
- EVENT(DELETEUSP)
- EVENT(R_SETUID)
- EVENT(R_SETEUID)
- EVENT(R_SETGID)
- EVENT(R_SETEGID)
- EVENT(INITACEE)
- EVENT(CK_ACCESS)

- EVENT(R_CHOWN)
- EVENT(R_CHMOD)
- EVENT(R_CHAUDIT)
- EVENT(R_AUDIT)
- EVENT(R_SETFACL)

NEWSYSID(*sysid*)

(Optional) Specifies an overriding system ID value that is inserted as the system ID value in each event record that gets loaded into the DB2 Data Mart repository. You cannot mask the NEWSYSID value. Specify only one NEWSYSID keyword in the SYSIN control statements. Do not abbreviate this optional keyword.

Limits: 1 to 8 character

Default: the system ID of the event record

POLICYSET(*policyset*)

(Optional) Specifies the name of the event policy set that the Data Mart uses to select events for unload. Do not abbreviate this optional keyword. Specify only one POLICYSET keyword in the SYSIN control statements.

Limits: 1 to 16 character, case-sensitive

Note: POLICYSET is mutually exclusive with the following input control statement keywords: EVENT, USERID, SYSID, and SYSPLEX.

SYSID(*sysid*)

(Optional) Specifies that logstream records be selected for unload based on a system ID. You cannot mask the SYSID value. Do not specify more than one SYSID keyword in the SYSIN control statements. Do not abbreviate this optional keyword.

Limits: 1 to 4 characters

Default: No selection occurs based on this field.

Note: SYSID and SYSPLEX are mutually exclusive. SYSID and POLICYSET are also mutually exclusive.

SYSPLEX(*sysplex*)

(Optional) Specifies that logstream records be selected for unload based on the name of a sysplex name. You cannot mask the SYSPLEX value. Specify only one SYSPLEX keyword in the SYSIN control statements. Do not abbreviate this optional keyword.

Limits: 1 to 8 characters

Default: No selection occurs based on this field.

Note: SYSID and SYSPLEX are mutually exclusive. SYSPLEX and POLICYSET are also mutually exclusive.

USERID(*userid*)

(Optional) Specifies that logstream event records be selected for unload based on a user ID field in a logstream event record. Do not abbreviate this optional keyword. You can specify more than one USERID keyword in the SYSIN control statements.

Limits: 1 to 8 characters

Default: No selection occurs based on this field.

Note: USERID and POLICYSET are mutually exclusive.

Sample Input control Statement Commands

The following examples show how to capture data on a specific date, daily basis, and in a specific time period.

Use the following example when capturing data on a specific date. For example, if today's date is 6/21/11, the following captures data from 12:00:00:01 a.m. on 6/21/11 to 11:59:59:99 p.m.

```
logstream(logstreamname)
SDATE(6/21/2011)
EDATE(6/21/2011)
```

Use the following example to automatically capture data on a daily basis. For example, if today's date is 6/21/2011, the following captures data today from 12:00:00:01 a.m. to 11:59:59:99 p.m. No specific date is required in this example.

```
logstream(logstreamname)
SDATE(TODAY)
EDATE(TODAY)
```

Use the following example to automatically capture data for the prior day. For example, if today's date is 6/21/2011, the following captures data from 12:00:00:01 a.m. to 11:59:59:99 p.m. on 6/20/2011. No specific date is required in this example.

```
logstream(logstreamname)
SDATE(TODAY-1)
EDATE(TODAY-1)
```

If you wish to capture data 20 days in the past from yesterday's date, indicate the following:

```
logstream(logstreamname)
SDATE(TODAY-20)
EDATE(TODAY-1)
```

Use the following example to automatically capture data in an 8-hour period of time. For example, if today's date is 6/21/2011, the following captures data today from 8:00 a.m. to 4:00 p.m.

```
logstream(logstreamname)
SDATE(TODAY)
STIME(08:00:00:00)
EDATE(TODAY)
ETIME(16:00:00:00)
```

Estimate the Space Requirements for the Data Mart Output Data Sets

Before you allocate the Data Mart UNLOAD DD, STATREPT DD, and ERRREPT DD output data sets, estimate the amount of space required for them.

Estimate the Amount of Storage Space for the UNLOAD DD Data Set

Before you allocate the Data Mart UNLOAD DD data set, estimate the amount of space required. Because this data set can contain large amounts of event data, it is critical that the data set is allocated with enough space to allow Data Mart unload processing to complete successfully.

Follow these steps:

1. Use the following equation to calculate the amount of space needed:

   (Total # of logstream records x 6,472 bytes) / 849,960 bytes =

   _____ Total space (in cylinders)

2. Determine how many records are in the system logstream that the Data Mart uses.

   You can query the Logger component, when it is active, with the F CMGRLOGR,STATUS console command to view the EventCount statistic. The statistic displays how many events the Logger component processed. For example, the following is a partial STATUS display, which shows the EventCount as 10,014 records the Logger component processed:

   ```
   CMGR240I  *** CMGR Logger Status ***
   CMGR240I    Logstream =        (CF) CMGR.CF.SYSLOG
   CMGR240I    Autodelete =        Yes
   CMGR240I    Retention =         1
   CMGR240I    Logrbufsize =       32768
   CMGR240I    Maxbufrsize =       65532
   CMGR240I    Logrbufrnum =       16
   CMGR240I    LogrActiveBufrNum = 1
   CMGR240I    LogStreamSize =     2 Mb
   CMGR240I    EventCount =        10014
   CMGR240I    WriteCount =        69
   CMGR240I    EventLostCount =    0
   ...
   ```

3. Multiply the total number of system logstream records by the maximum UNLOAD data set security event record length (6,472 bytes), to determine the maximum number of bytes of storage needed for the data set.
4. Divide the total number of bytes of storage needed by the number of bytes on a cylinder for the hardware disk model you are using, to determine the total number of cylinders of space to allocate.

   Note: IBM disk model 3390 has 849,960 bytes per cylinder.

Estimate the Amount of Storage Space for the STATREPT DD Data Set

The STATREPT DD data set requires a small amount of space.

Allocate enough space to hold several printed pages of Data Mart summary statistical information.

Estimate the Amount of Storage Space for the ERRREPT DD Data Set

The ERRREPT DD data set requires space to hold the error information for invalid security event records. These are records that the Data Mart reads from the system logstream but does not unload. Most likely, there are few, if any, invalid security event records. However, we recommend that you initially plan to accommodate error information for all logstream security event records.

Follow these steps:

1. Estimate the total space for the ERRREPT DD data set by multiplying the space parameter for the UNLOAD DD data set by two.
2. After CMGRDUNL job runs for the first time, if necessary, you can reallocate the ERRREPT DD data set with a space parameter that more accurately reflects your installation's needs.

Allocate the Data Mart Output Data Sets

After you estimate the space needed for the Data Mart output data sets, you can allocate them. The CMGRDALC job allocates the following output data sets for the Data Mart:

UNLOAD DD

Contains the security event information that the Data Mart unloaded from the system logstream.

STATREPT DD

Contains Data Mart statistical information and errors that caused the Data Mart to terminate before successful completion.

ERRREPT DD

Contains information about each invalid event record the Data Mart encounters.

Follow these steps:

1. Edit the CMGRDALC job in CAI.CEIQJCL0.

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and Customization sections of the job to customize the job for your environment.
2. Modify the space parameters for the UNLOAD DD, STATREPT DD, and ERRREPT DD data sets based on your estimates.
3. Submit the CMGRDALC job.
4. Review the job output.

   Verify that the UNLOAD DD, STATREPT DD, and ERRREPT DD data sets were successfully created.

Unload Data from the Logstream using the Data Mart

The CMGRDUNL job executes the Data Mart, which unloads selected security event information from the system Logger logstream into the UNLOAD DD data set.

Follow these steps:

1. Edit the CMGRDUNL job in CAI.CEIQJCL0 library.

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and Customization sections of the job to customize the job for your environment.
2. Specify the UNLOAD DD output data that contains the security event information extracted from the system logstream. This data is unloaded in a format for the DB2 Load Utility to load to the Data Mart repository.

3. Specify the ERRREPT DD error report output data set. The Data Mart writes the following information into this file:
   - General information about the event record
   - The reason why the event record is invalid
   - A hexadecimal dump of the event record
4. Specify the STATREPT DD Data Mart statistical report output data set. The Data Mart writes the following information to this file:
   - Statistical summary information about the unload process
   - Errors that caused the Data Mart to terminate before successful completion
5. Specify the MAPDB DD parameter, even if you do not specify the SYSIN DD file POLICYSET input control statement.

   This is the name of the data set that was configured in CA LDAP Server as the CA Compliance Manager event policy database (policy file). The policy file holds the event policy. For more information about how to configure the policy file for use by CA Compliance Manager, see the CA LDAP Server for z/OS *Installation Guide*. See also Configure CA LDAP Server for z/OS and CA Compliance Manager (see page 136).
6. Specify the following required SYSIN DD input control statements. These statements select each security event record from the logstream that matches the Data Mart event selection criteria:
   - LOGSTREAM(*logstream*)
   - SDATE(*mm/dd/yyyy*|TODAY|TODAY-*nnnn*)
   - EDATE(*mm/dd/yyyy*|TODAY|TODAY-*nnnn*)
7. Specify any other SYSIN DD file input control statements that you require to conform to your site's standards.
8. Submit the job.

9. Check the output of the CMGRDUNL job. Verify that the Data Mart completes successfully.

   The Data Mart returns the following codes for the unload process:

   0 - Indicates that the unload process was successful.

   12 - Indicates that the unload process failed (The Data Mart issues a diagnostic message).

   If the Data Mart encounters an invalid event record, it continues processing the next event record in the logstream without terminating. Before continuing, it reports the invalid record in the ERRREPT DD data set.

   If the CMGRDUNL job fails for any reason, review the error in the STATREPT DD data set, fix the error, and rerun the job until it successfully completes. Otherwise, the UNLOAD DD data set cannot properly be loaded into the DB2 Data Mart repository and the data will not be available for compliance analysis.

Load the CA Datacom/AD Data Mart Repository

If you implement a CA Datacom/AD Data Mart repository, the CMGRDLDC job converts the unloaded ESM security events from DB2 load format to CA Datacom/AD load format. It also separates them into different data sets by target table as required by the CA Datacom/AD load process. It then loads the security events into the CA Datacom/AD Data Mart repository.

Perform the following steps to complete the CA Datacom/AD conversion and load process:

- Estimate the storage space requirements for the conversion output data sets.
- Execute the Data Mart CA Datacom/AD Conversion Utility.
- Review the Data Mart CA Datacom/AD Conversion Utility Report.

Estimate the Storage Space for Data Mart CA Datacom/AD Conversion Utility Output Data Sets

The first step of the CMGRDLDC job converts the information in the UNLOAD data set from a DB2 load format into a CA Datacom/AD load format. This data set is created by the Data Mart unload utility.

The CMGRDLDC job then separates the data sets by target table as required by the CA Datacom/AD load process. The following statements define these data sets in the job:

ADMACCOUNT DD

Specifies the output data set where data converted to CA Datacom/AD load format is placed for the CA Datacom/AD Data Mart repository ADMACCT table.

ADMMISC DD

Specifies the output data set where data that is converted to CA Datacom/AD load format is placed for the CA Datacom/AD Data Mart repository ADMMISC table.

ADMPOLICY DD

Specifies the output data set where data that is converted to CA Datacom/AD load format is placed for the CA Datacom/AD Data Mart repository ADMPOL table.

OBJACCESS DD

Specifies the output data set where data that is converted to CA Datacom/AD load format is placed for the CA Datacom/AD Data Mart repository OBJACC table.

SECCONTROL DD

Specifies the output data set where data that is converted to CA Datacom/AD load format is placed for the CA Datacom/AD Data Mart repository SECCTRL table.

SYSACCESS DD

Specifies the output data set where data that is converted to CA Datacom/AD load format is placed for the CA Datacom/AD Data Mart repository SYSACC table.

USSFILE DD

Specifies the output data set where data that is converted to CA Datacom/AD load format is placed for the CA Datacom/AD Data Mart repository USSFILE table.

USSUSER DD

Specifies the output data set where data that is converted to CA Datacom/AD load format is placed for the CA Datacom/AD Data Mart repository USSUSER table.

These data sets can contain large amounts of event data. Because of this, data sets must be allocated with enough space to allow Conversion Utility processing to complete.

Follow these steps:

1. Use the following equation to calculate the amount of space that is needed for each output data set:

   Total number of DB2 load table records x [(6,395 bytes) [OR] (max record length of a table record)] / 849,960 bytes = _____ Total space (in cylinders)

2. Review the Data Mart Statistical Report to find the total load records generated in the Data Mart Unload DD data set.

3. Multiply the total number of unloaded records by the maximum Data Mart CA Datacom/AD table record length (6395 bytes). This determines the maximum number of bytes of storage that is needed for each CA Datacom/AD output data set.

   Note: To more accurately determine the amount of space to allocate, use the maximum record lengths for each CA Datacom/AD load table that is listed in the following table.

CA Datacom/AD Load Data Set	Maximum Record Length
ADMACCOUNT DD	4547
ADMMISC DD	4529
ADMPOLICY DD	4759
OBJACCESS DD	6395
SECCONTROL DD	4473
SYSACCESS DD	416
USSFILE DD	1730
USSUSER DD	440

4. Divide the total number of bytes of storage needed by the number of bytes on a cylinder. The number of bytes per cylinder depends on the hardware disk model you are using. IBM disk model 3390 has 849,960 bytes per cylinder.

   You have determined the total number of cylinders of space to allocate for each CA Datacom/AD load format data set.

Execute the Data Mart CA Datacom/AD Conversion Utility

The CMGRDLDC job in the CAI.CEIQJCL0 library converts the UNLOAD DD data set information, which is in DB2 load format into CA Datacom load format and loads the information into the CA Datacom Data Mart repository.

The CMGRDLDC job consists of the following steps:

DELETE.

Deletes existing CA Datacom load format data sets.

CONVERT.

Executes the ECADMDCC conversion utility to convert the unload data set into the appropriate CA Datacom load format data sets. This unload data set is created by the CMGRDUNL job.

CLEARDB.

Deletes any information currently in the Data Mart repository tables.

Note: The CLEARDB step of this job deletes all existing data in the current Data Mart repository tables. To add new data to an existing Data Mart repository, remove the CLEARDB step from the job before execution.

LOAD.

Executes the CA Datacom DBUTLTY program to load the security information into the Data Mart repository tables.

CONTBLS.

Inserts constant information into the constant value tables in the Data Mart repository.

Follow these steps:

1. Edit the CMGRDLDC job in CAI.CEIQJCL0.

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and Customization sections of the job to customize the job for your environment.

2. Modify the space parameters in the CONVERT step for each CA Datacom/AD load format data set based on your estimates. See Estimate the Storage Space for Data Mart CA Datacom/AD Conversion Utility Output Data Sets.

3. Add new data to an existing Data Mart repository by removing the CLEARDB step from the job before execution.

   The CLEARDB step of this job deletes all existing data in the current Data Mart repository tables.

4. Specify the Data Mart Selection Utility UNLOAD DD output data set that contains security event information in DB2 Load Utility format. The Data Mart CA Datacom/AD Conversion Utility converts this information into CA Datacom/AD load format.

5. Specify the Data Mart CA Datacom/AD Conversion Utility (REPORT DD) Statistical Report output data set.

   The Utility writes the following information to this file:

   - Statistical summary information about the DB2 to CA Datacom/AD load format conversion process
   - Errors that caused the Utility to terminate before successful completion

6. Submit the job.

   The job executes and completes.

7. Verify the output of the CMGRDLDC job.

   Check the output of the CMGRDLDC job, verifying that the security event information has been loaded successfully.

   Note: If the CMGRDLDC job fails for any reason, review the error in the Data Mart CA Datacom/AD Conversion Utility Report (REPORT DD) output data set, fix the error, and rerun the job until it successfully completes. The job must successfully complete for the output data sets to load properly into the Data Mart CA Datacom/AD repository.

Review the Data Mart CA Datacom/AD Conversion Utility Report

The Data Mart CA Datacom/AD Conversion Utility writes summary statistical information about the conversion process and errors that cause processing to terminate to the REPORT DD data set that was allocated before the Utility was run.

The following is an example of report output generated by the Data Mart CA Datacom/AD Conversion Utility:

```
Compliance Manager Data Mart CA Datacom/AD Conversion Report Page 1
Date 12/31/09 (09.365) Time 11.27

ADMACCOUNT      record count                  4,547
ADMMISC         record count                  4,529
ADMPOLICY       record count                  4,759
OBJACCESS       record count                  6,395
SECCONTROL      record count                  4,473
SYSACCESS       record count                    416
USSFILE         record count                  1,730
USSUSER         record count                    440
```

ADMACCOUNT records selected nnnnnnnnnn

Identifies the number of ADMACCOUNT event records converted from DB2 to CA Datacom/AD load format.

ADMMISC records selected nnnnnnnnnn

Identifies the number of ADMMISC event records converted from DB2 to CA Datacom/AD load format.

ADMPOLICY records selected nnnnnnnnnn

Identifies the number of ADMPOLICY event records converted from DB2 to CA Datacom/AD load format.

OBJACCESS records selected nnnnnnnnnn

Identifies the number of OBJACCESS event records converted from DB2 to CA Datacom/AD load format.

SECCONTROL records selected nnnnnnnnnn

Identifies the number of SECCONTROL event records converted from DB2 to CA Datacom/AD load format.

SYSACCESS records selected nnnnnnnnnn

Identifies the number of SYSACCESS event records converted from DB2 to CA Datacom/AD load format.

USSFILE records selected nnnnnnnnnn

Identifies the number of USSFILE event records converted from DB2 to CA Datacom/AD load format.

USSUSER records selected nnnnnnnnnn

Identifies the number of USSUSER event records converted from DB2 to CA Datacom/AD load format.

Load the DB2 Data Mart Repository

If you implement a DB2 Data Mart repository, the CMGRDL00 job executes the DB2 Load Utility to load the security information from an UNLOAD DD data set into the DB2 Data Mart repository in the target DB2 subsystem. It executes a series of steps to load and replace the entire DB2 Data Mart repository.

The CMGRDL00 job refers to the following other jobs in CAI.CEIQJCL0. These jobs contain the scripts to load the security event information from the UNLOAD DD data set into each table in the DB2 Data Mart repository:

CMGRDLAA

Loads the ADMACCOUNT target table

CMGRDLAM

Loads the ADMMISC target table

CMGRDLAP

Loads the ADMPOLICY target table

CMGRDLOA

Loads the OBJACCESS target table

CMGRDLSA

Loads the SYSACCESS target table

CMGRDLSC

Loads the SECCONTROL target table

CMGRDLUF

Loads the USSFILE target table

CMGRDLUU

Loads the USSUSER target table

Follow these steps:

1. Edit the CMGRDL00 job in CAI.CEIQJCL0 to conform to your installation standards. Direct it to the target DB2 subsystem where the DB2 Data Mart repository is defined.
2. Modify the job to conform to your installation standards. Follow the instructions in the Notes and Customization sections of the job to customize the job for your environment.

   Important! The DB2 LOAD Utility requires DFSORT. If DFSORT is not your default sort program, add a STEPLIB to the CMGRDL00 or CMGRDA00 job to specify the correct libraries where DFSORT resides.

3. Submit the job.
4. Check the output of the CMGRDL00 job to verify that the security information has been loaded successfully.

   Note: Run the CMGRDL00 job each time you run the Data Mart to replicate the most current information in the DB2 Data Mart repository.

Load Additional Data Into an Existing DB2 Data Mart Repository

You may need to load additional security information from an UNLOAD DD data set into an existing Data Mart repository without deleting or replacing any of the existing data. Unlike the CMGRDL00 job, which loads and replaces the entire DB2 Data Mart repository, the CMGRDA00 job executes a series of steps to load additional security information into an existing DB2 Data Mart repository in the target DB2 subsystem without replacing any data.

The CMGRDA00 job in CAI.CEIQJCL0 refers to the following other jobs in CAI.CEIQJCL0. These jobs contain the scripts to load the security event information from the UNLOAD DD data set into each table in the DB2 Data Mart repository:

CMGRDAAA

Loads the ADMACCOUNT target table

CMGRDAAM

Loads the ADMMISC target table

CMGRDAAP

Loads the ADMPOLICY target table

CMGRDAOA

Loads the OBJACCESS target table

CMGRDASA

Loads the SYSACCESS target table

CMGRDASC

Loads the SECCONTROL target table

CMGRDAUF

Loads the USSFILE target table

CMGRDAUU

Loads the USSUSER target table

Follow these steps:

1. Edit the CMGRDA00 job in CAI.CEIQJCL0. Direct it to the target DB2 subsystem where the DB2 Data Mart repository is defined.

   Modify the job to conform to your installation standards. Follow the instructions in the Notes and Customization sections of the job to customize the job for your environment.

   Important! The DB2 LOAD Utility requires DFSORT. If DFSORT is not your default sort program, add a STEPLIB to the job to specify the correct libraries where DFSORT resides.

2. Submit the job.

3. Verify that the security information has been loaded successfully by checking the output of the CMGRDA00 job.

   Note: Run the CMGRDA00 job each time you run the Data Mart to add the most current information to the DB2 Data Mart repository.

Appendix A: Site Preparation Worksheet

This worksheet contains basic information for the data sets, jobs, and variables that are required for the CA Chorus for Security and Compliance Management discipline. Use this worksheet to help you understand, customize, and record your values to reference during the site preparation process. For complete information on how to incorporate them into your installation process, follow the instructions in this guide.

This section contains the following topics:

Part 1 - Basic Information

Record the following values for part 1 of the Site Preparation Worksheet:

- CA product installation library values for the high-level qualifiers of installation data sets
- Started task procedures values
- CA LDAP Server and CA DSI Server values
- CIA Real-Time Component values
- CA Compliance Manager values

CA Product Installation Library Values

Record the following high-level qualifiers of installation data sets.

High-level (HLQ) for the CA Common Services for z/OS (CCS) installation data sets

Default: CAI

Your Value _____

HLQ of installation data sets for CA Chorus Version 3.0

Default: *your_chorus_hlq*

Example: CAI.CHORUS.V300

Your Value _____

HLQ of installation data sets for CA Chorus for Security and Compliance Management discipline

Default: *your_chorussec_hlq*

Example: CAI.CHORUS.V300

Your Value _____

HLQ of installation data sets for CA ACF2 Version 15

Default: CAI

Example: CAI.ACF2.V150

Your Value _____

HLQ of installation data sets for CA Top Secret Version 15

Default: CAI

Example: CAI.TOPSECRT.V150

Your Value _____

HLQ of installation data sets for CA LDAP Server Release 15.1

Default: *your_ldap_hlq*

Example: CAI.LDAP.V151

Your Value _____

HLQ of installation data sets for CA DSI Server Release 15.1

Default: *your_ldap_hlq*

Example: CAI.LDAP.V151

Your Value _____

HLQ of installation data sets for CA Datacom/AD Version 14

Default: *your_datacom_hlq*

Example: CAI.DCOM.V140

Your Value _____

HLQ of installation data sets for CA Compliance Manager Version 2.0

Default: CAI

Example: CAI.CACMGR.V200

Your Value _____

Started Task Procedures

Started Task Procedure for RRSAF (DB2 only)

Example: RRS

Your Value: _____

Started Task Procedure for DB2 (DB2 only)

Example: DB2START

Your Value: _____

Started Task Procedure for CA LDAP Server

Example: LDAPR15

Your Value: _____

Started Task Procedure for CA DSI Server

Example: DSIR15

Your Value: _____

Started Task Procedure for CA Datacom/AD MUF for CIA real-time component

Example: CIAMUF

Your Value: _____

Started Task Procedure for CA Datacom/AD Server for CIA

Example: CIASRV

Your Value: _____

Started Task Procedure for CIA real-time component

Example: CIARTUPD

Your Value: _____

Started Task Procedure for CA Datacom/AD MUF for CA Compliance Manager

Example: CMGRMUF

Your Value: _____

Started Task Procedure for CA Datacom/AD Server for CA Compliance Manager (CA Datacom/AD only)

Example: CMGRSRV

Your Value: _____

Started Task Procedure for CA Compliance Manager Router

Example: CMGRRTR

Your Value: _____

Started Task Procedure for CA Compliance Manager Alert component

Example: CMGRALRT

Your Value: _____

Started Task Procedure for CA Compliance Manager Logger Component

Example: CMGRLOGR

Your Value: _____

Started Task Procedure for CA Compliance Manager Warehouse Component

Example: CMGRWHSE

Your Value: _____

Started Task Procedure for CA Compliance Manager Monitor Component

Example: CMGRMON

Your Value: _____

CA LDAP Server and CA DSI Server Values

Record the following values for CA LDAP Server and CA DSI Server.

Name or IP address of the system running the CA LDAP Server

(defined in: /usr/lpp/caldapr151/slapd.conf)

Default: LPAR name or IP Address

Example: 111.111.111.111

Your Value _____

TCP/IP port that CA LDAP Server is using

(defined in: /usr/lpp/caldapr151/slapd.conf)

Default: Port number

Example: 389

Your Value _____

Values that allow CA LDAP Server and CA Chorus for Security and Compliance Management to communicate

(defined in: /usr/lpp/caldapr151/slapd.conf)

Default: LPAR suffix

Example: o=ca,c=us

Your Value _____

CIA Real-Time Component Values

Record the following values for CIA Real-Time Components.

CA Datacom/AD Values for CIA Repository

Record the following values for the CA Datacom/AD CIA Repository.

CA Datacom/AD load library for the CA Datacom/AD system where the CIA database is installed

Variable: DCOMLOADCIA

Default: CAI.CAAXLOAD

Example: DCOM.V140.CAAXLOAD

Your Value: _____

CA Datacom/AD MUF CUSLIB library for the CA Datacom/AD system where the CIA database is installed

Variable: DCOMCUSCIA

Default: CAI.MUF.CUSLIB

Example: DCOM.V140.CIAMUF.CUSLIB

Your Value: _____

CA Common Services for z/OS (CCS) library for the CA Datacom/AD system where the CIA database is installed

Variable: DCOMCCSCIA

Default: CAI.CAW0LOAD

Your Value: _____

DB2 Values for CIA Repository

Record the following DB2 values for the CIA Repository.

DB2 subsystem name where the CIA database is located

Variable: SSIDCIA

Default: DB2

Example: D10A

Your Value: _____

SDSNLOAD library for the DB2 system where the CIA database is defined

Variable: SDSNLOADCIA

Default: DB2.SDSNLOAD

Example: D10A.SDSNLOAD

Your Value: _____

RUNLIB library for the DB2 system where the CIA database is defined (RUNLIB contains DSNTIAD and DSNTEP2)

Variable: RUNLIBCIA

Default: DB2.RUNLIB.LOAD

Example: D10A.RUNLIB.LOAD

Your Value: _____

WLM environment used for function execution

Variable: DSNWLM

Default: DSNWLM

Example: D10AWLM

Your Value: _____

Database that was created to contain the CIA tables

Variable: CIADB01

Default: CIADB01

Your Value: _____

Storage group qualifier that is used for the CIA database

Variable: CIASG01

Default: CIASG01

Your Value: _____

Plan name that is bound to DSNTIAD on the DB2 subsystem with the CIA database

Variable: DSNTIAxx

Default: DSNTIA??

Example: DSNTIA10

Your Value: _____

Buffer pool value for the DB2 subsystem

Variable: BP0

Default: BP0

Your Value: _____

Plan name that is bound to DSNTEP2 on the DB2 subsystem with the CIA database

Variable: DSNTEPxx

Default: DSNTEP??

Your Value: _____

Other CIA Real-Time Values

Record the following other CIA Real-time values.

CIA Logstream Name

Default: CIA.*sysid*.DASD.LOGST

Your Value: _____

Name of CIA Real-Time Status Data Set

Default: CAI.CIART.STATUS

Your Value: _____

Name of CIA Real-Time Journal Data Set

Default: CAI.CIART.JOURNAL

Your Value: _____

Name of CIA Unload Data Set (UNLOAD DD)

Default: HLQ.CIAUNLD.UNLOAD

Your Value: _____

Name of CA Datacom/AD Load Format Data Sets

Default: HLQ.CIADCOM.UNLOAD

Your Value: _____

Name of CA Top Secret TSSCFILE Output Data Set

Default: HLQ.CIAUNLD.UNLOAD

Your Value: _____

CA Compliance Manager Values

Record the following values for CA Compliance Manager components.

CA Datacom/AD Values for CA Compliance Manager Repositories

Record the following CA Datacom/AD values for the CA Compliance Manager repositories.

CA Datacom/AD utility load library for the CA Datacom/AD system where the CA Compliance Manager database is installed

Variable: DCOMLOADCM

Default: DCOM.V140.CAAXLOAD

Example: CAI.DCOM.V410.CAAXLOAD

Your Value: _____

CA Datacom/AD MUF CUSLIB library for the CA Datacom/AD system where the CA Compliance Manager database is installed

Variable: DCOMCUSCM

Default: DCOM.V140.MUF.CUSLIB

Example: DCOM.V140.CMGRMUF.CUSLIB

Your Value: _____

CA Common Services library for the CA Datacom/AD system where the CA Compliance Manager database is installed

Variable: DCOMCCSCM

Default: CAI.CAW0LOAD

Your Value: _____

DB2 Values for CA Compliance Manager Repositories

Record the following DB2 values for the CA Compliance Manager repositories.

DB2 subsystem name where the CA Compliance Manager database is located

Variable: SSIDCM

Default: DB2

Your Value: _____

SDSNLOAD library for the DB2 system where the CA Compliance Manager database is defined

Variable: SDSNLOADCM

Default: DB2

Example: D10A.SDSNLOAD

Your Value: _____

RUNLIB library for the DB2 system where the CA Compliance Manager database is installed (RUNLIB contains DSNTIAD and DSNTEP2)

Variable: RUNLIBCM

Default: DB2.RUNLIB.LOAD

Example: D10A.RUNLIB.LOAD

Your Value: _____

Qualifier used for the Data Mart database in CA Compliance Manager

Variable: CMGRD1

Default: CMGRD1

This value must match the CA Compliance Manager table qualifier. The table qualifier is the first part in a qualified table name. For example, if the table name is CMGRD1.ADMACCOUNT, CMGRD1 is the qualifier.

The CA Compliance Manager tables are defined by CMGRIDB2 job in the CA Compliance Manager JCL library. If you are unsure of the value to specify for this qualifier, verify through the CMGRIDB2 job and your DBA the value to use.

Your Value: _____

Plan name bound to DSNTEP2 on the DB2 subsystem with the CA Compliance Manager database

Variable: DSNTEPyy

Default: DSNTEP??

Your Value: _____

Other CA Compliance Manager Values

Record the other values associated with the CIA Real-Time component.

CA Compliance Manager Logger Component DASD-Only Logstream Name

Default: HLQ.DASD.LGSTRM

Example: CMGRLG.DASD.LGSTRM

Your Value: _____

CA Compliance Manager Logger Component C.F. Based Logstream Name

Default: HLQ.CF.LGSTRM

Example: CMGRLG.CF.LGSTRM

Your Value: _____

Names of CA Compliance Manager Component Default Policy Sets

Default (Alert): POLICYSET=ALERTPOLICY

Default (Logger): POLICYSET=VIOLATIONS

Default (Warehouse): POLICYSET=VIOLATIONSDW

Default (Monitor): POLICYSET=MONITOR

Names of CA Compliance Manager Component Status Data Sets

Default: CAI.CMGRRTR.STATUS

Your Value: _____

Default: CAI.CMGRALRT.STATUS

Your Value: _____

Default: CAI.CMGRLOGR.STATUS

Your Value: _____

Default: CAI.CMGRWHSE.STATUS

Your Value: _____

Default: CAI.CMGRMON.STATUS

Your Value: _____

Names of CA Compliance Manager Component Journal Data Sets

Default: CAI.CMGRALRT.JOURNAL

Your Value: _____

Default: CAI.CMGRMON.JOURNAL

Your Value: _____

Name of Data Mart Unload Data Set (UNLOAD DD)

Default: CAI.CMGRDMRT.UNLOAD

Your Value: _____

Name of Data Mart Status Report Data Set (STATREPT DD)

Default: CAI.CMGRDMRT.STATREPT

Your Value: _____

Name of Data Mart Status Report Data Set (ERRREPT DD)

Default: CAI.CMGRDMRT.ERRREPT

Your Value: _____

Name of Data Mart MAPDB Data Set (MAPDB DD) (this is the Policy File database name)

Default: HLQ.MAPDB

Your Value: _____

High-level qualifier of Data Mart CA Datacom/AD Load Format Data Sets

Default: MARTDCOM.UNLOAD

Your Value: _____

Part 2 - List of Jobs

The jobs, files, and elements in part 2 of Site Preparation Worksheet appear in the following order in which they are configured and run during the CA Chorus for Security and Compliance Management discipline site preparation process.

- Addressing security requirements
- Configuring CA LDAP Server and CA DSI Server
- Implementing CIA Real-Time for CA Chorus for Security and Compliance Management
- Implementing CA Compliance Manager for CA Chorus for Security and Compliance Management

Addressing Security Requirements

The following jobs address the security requirements required when installing the CA Chorus for Security and Compliance Management discipline.

Define Security Authorizations for CA Chorus for Security and Compliance Management

E1MIA021 | E1MIT021

Configures CA ACF2 (E1MIA021) and CA Top Secret (E1MIT021) security authorizations for the CA Chorus for Security and Compliance Management discipline.

- Defines CA Chorus installer user id privileges for:
  - UNIX System Services (USS)
  - z/OS
- Authorizes CA Chorus users to access USS resources
- Authorizes users to work in CA Chorus
- Configures PassTickets for user authentication

E1MIA021

Provides commands for CA ACF2.

E1MIT021

Provides commands for CA Top Secret.

Define Security Authorizations for CA LDAP Server

CDT9ACID|CDT9LID

Creates the security environment for the CA LDAP Server component and defines the following:

- Started task ID for the CA LDAP Server component as well as its department and group ID
- Permissions to data sets (such as TCP/IP)
- Facility accesses for BPX server and daemon

CDT9LID

Provides commands for CA ACF2.

CDT9ACID

Provides commands for CA Top Secret.

CA LDAP Server: *your_ldap_hlq*.CDT9JCL

LDAPR15

Started task procedure for CA LDAP Server.

CA LDAP Server: *your_ldap_hlq*.CDT9JCL

Define the Started Task User ID for CA DSI Server

DSILID | DSIACID

Creates the started task user id for CA DSI Server installation.

DSILID

Provides commands for CA ACF2.

DSIACID

Provides commands for CA Top Secret.

CA LDAP Server: *your_ldap_hlq*.CDT9JCL

DSIR15

Started task procedure for the CA DSI Server.

CA DSI Server: *your_ldap_hlq*.CDT9JCL

dsi.env

Environment file for the CA DSI Server.

Default location of file: /usr/lpp/caldapr151

dsi.conf

Configuration file for CA DSI Server.

Default location of file: /usr/lpp/caldapr151

Define Security Authorizations for CA DSI Server

DSICIA

Defines the security authorizations for CA DSI Server to enable the server to access the CIA repository. It assigns the CA DSI Server authorization to access the CA Datacom/AD or DB2 database plan. When CIA real-time processing is implemented, a CIA plugin module in the CA DSI Server performs processing against the CIA repository.

CA DSI Server: *your_ldap_hlq*.CDT9JCL

PassTicket Configuration to Connect to CA Datacom/AD

CA Datacom/AD Server PROC

CA Datacom/AD Server started task procedure created during the CA Chorus platform installation.

STEPLIB

STEPLIB concatenation for the CA Datacom/AD Server PROC.

***your_chorus_hlq*.CETJPLD**

Target library from the CA Chorus platform installation.

Configure CA LDAP Server Resource Authorizations for CA Compliance Manager Policies and Reports

slapd.conf

This is the configuration file for CA LDAP Server in which the names of the CA Compliance Manager policies and reports resource names can be customized for authorizations.

Default location of file: /usr/lpp/caldapr151

Define Security Authorizations for CIA Real-Time Component (CA ACF2)

CIARTACF

This job defines the CA ACF2 security authorizations for the CIA Real-Time component, including the following:

- Defines an STC logonid for the CIA real-time component address space with the unscoped AUDIT privilege and defines the OMVS and group profiles required for USS capabilities.
- Gives the STC logonid access to the CIA real-time component data sets.
- Defines the CIA real-time GSO CHORUS record.

CA ACF2: CAI.CAX1JCL0

Define Security Authorizations for CIA Real-Time Component (CA Top Secret)

CIARTTSS

Defines the CA Top Secret security authorizations for the CIA Real-Time Component, including the following:

- Creates the STC ACID with unscoped control authority (type SCA)
- Gives the ACID administrative authorities and permissions required to run CIA real time
- Defines the OMVS and group profiles required for USS capabilities
- Assigns the STC ACID to the CIA real-time task in the STC

CA Top Secret: CAI.CAK0JCL0

Define the Security Authorizations for CIA Real-Time CA Datacom/AD MUF

CIASECC

Creates the security authorizations for the CIA Real-Time CA Datacom/AD MUF and the CIA repository as well as the authorizations for the users who access the CIA repository.

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

Define Security Authorizations for CA Compliance Manager

CMGRIACF | CMGRITSS | CMGRIRAC

Defines the CA ACF2, CA Top Secret, or IBM RACF security environment for all of the CA Compliance Manager components by creating the security definitions for the CA Datacom/AD MUF and the CA Compliance Manager repositories and the authorizations for the users who access the repositories.

CA Compliance Manager: CAI.CEIQJCL0

CAI.CEIQLOAD

The APF-authorized library in which the CA Compliance Manager ECARTINT program resides. The Router does not initialize if it is executed from an unauthorized library.

CA Compliance Manager: CAI.CEIQLOAD

Configuring CA LDAP Server and CA DSI Server

The following jobs address the security requirements for configuring CA LDAP Server and CA DSI Server.

Define Security Authorizations for CA Compliance Manager

slapd.conf

The configuration file for CA LDAP Server, in which the following required values exist for the CA Compliance Manager interface installation procedure:

LPAR name or IP Address

Defines the name or IP address of the system running the CA LDAP Server.

Port number

Specifies the TCP/IP port that CA LDAP Server is using.

Example: 389

LDAP suffix

Specifies the values that let CA LDAP Server and CA Chorus for Security and Compliance Management communicate; these values identify the back-end.

Example: o=ca,c=us

Default location of file: /usr/lpp/caldapr151

Implementing CIA Real-Time for CA Chorus for Security and Compliance Management

The following jobs and elements address the security requirements for implementing CIA Real-Time for CA Chorus for Security and Compliance Management.

Create the CA Datacom/AD MUF for CIA Real-Time

AXCUS00

Creates the *your_datacom_hlq*.INSTJCL data set and copies members so they can be modified by the site. It builds, populates, and mass-edits the installation JCL data set.

CA Datacom/AD: *your_datacom_hlq*.CAAXSAMP

AXCUS01

Includes all customization for the CIA CA Datacom/AD MUF.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

AXNEW01

Allocates and populates data sets that the CA Datacom/AD MUF needs.

CA Datacom/AD: *your.datacom.hlq.*INSTJCL

AXRIM01

Installs the PC CALLS.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

AXAPFADD

Provides a CA SYSVIEW example to dynamically add libraries to be APF listed.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

AD14STRT

Creates the started task procedure that starts the test instance of the CIA real-time CA Datacom/AD MUF

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

AXIVP01

Sample install verification job.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

AD14STOP

Stops the test instance of the CIA real-time CA Datacom/AD MUF.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

Link the CIA Functions with CA Datacom/AD

CIALINKC

Links the CIA service function modules with CA Datacom/AD entry modules.

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

Delete the CIA Repository for CA Datacom/AD (If Required)

CIADCOMD

This job deletes an existing CIA repository, if required, so it can be redefined.

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

Define the CIA Repository for CA Datacom/AD

CIADCOM

Defines the CIA application and repository to CA Datacom/AD. Within the job are individual job steps that perform the following:

- Allocate the data sets to hold the CIA repository database
- Define the CIA database to the CA Datacom/AD data dictionary
- Initialize the CIA database
- Import the CIA database table and index definitions
- Import the application plans for the CIA service functions and procedure
- Create the CIA service functions and procedure

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

Link the DB2 Modules Into Functions

CIA4LNK1

Links the DB2 modules, DSNRLI and DSNTIAR, into the service functions in the target DB2 subsystem with the CIA security repository.

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

Delete the CIA Repository for DB2 (If Required)

CIADB2D

Deletes an existing CIA repository so it can be redefined, if required.

Define the CIA Repository for DB2

CIADB2

Performs the tasks of defining the CIA application and repository to DB2. Within the job are individual job steps that do the following:

- Define the CIA database, table spaces, tables, and indexes that comprise the security repository.
- Define the CIA service functions
- Define the CIA stored procedures
- Bind the application packages that correspond to the service functions

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

Configure CA DSI Server for CIA Real-Time

dsi.conf

Configuration file for CA DSI Server, which is modified to specify the DB2 subsystem (ssid) or CIA CA Datacom/AD MUF name (CIAMUF).

Default location of file: /usr/lpp/caldapr151

SDSNLOAD dataset

If using DB2, this is the DB2 data set specified in the STEPLIB concatenation for the CA DSI Server started task (dsi.env) . For example:

//STEPLIB DD DSN=DSN910.SDSNLOAD,DISP=SHR

CUSLIB dataset

If using CA Datacom/AD, this is the data set specified in the STEPLIB concatenation for the CA DSI Server started task (dsi.env). For example:

```
//STEPLIB DD DSN=DATACOM.CUSLIB,DISP=SHR
```

STEPLIB DD

The STEPLIB concatenation for the CA DSI Server started task (dsi.env).

CA DSI Server: *your_ldap_hlq*.CDT9JCL

Define the CIA Real-Time Logstream

CIALOGST

Defines the CIA real-time dedicated logstream, which records update requests made to any security product information that is replicated in the CIA repository. The CIA real-time component reads this logstream and communicates the update requests to the CIA repository.

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

CIAALLOC

Allocates the CIA UNLOAD DD data set that contains the CIA security data unloaded from the ESM.

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

Run TSSFAR Utility (CA Top Secret Only)

TSSFAR

Executes the TSSFAR Utility to validate the security file for CIA before security data is unloaded from CA Top Secret.

CA Top Secret: CAI.CAK0JCL0

Run the CIACFILE Job (CA Top Secret Only)

CIACFILE

Executes TSSCFILE. The TSSCFILE output is used as input into the CIA Unload Utility to generate data to be loaded into a DB2 CIA database.

CA Top Secret: CAI.CAK0JCL0

Run the CIA Unload Utility

CIAUNLD

Executes the CIA unload utility, which reads information from the security database and creates an UNLOAD data set. The UNLOAD data set contains data in DB2 load format that is loaded into the CIA repository.

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

Load the Security Information Into a CA Datacom/AD Repository

CIALOADC

Converts the unloaded CIA security information from DB2 load format into CA Datacom/AD load format and separates the converted records into individual data sets by table as required by the CA Datacom/AD load process. It then executes the CA Datacom/AD DBUTLTY program to load the security information into the CIA repository tables.

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

Load the Security Information Into DB2

CIALOAD

Executes a series of steps to initially load security information into the CIA repository in the target DB2 subsystem.

Important! This job replaces all existing data in the CIA repository.

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

CIALOADA

This job executes a series of steps to load additional security information into an existing CIA repository in the target DB2 subsystem. It is run for each subsequent load after the CIALOAD job is run, so the existing CIA data is retained in the Repository.

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

Allocate the CIA Real-Time Output Data Sets

CIARTALC

Allocates the CIA real-time status and journal output data sets. The CIA real-time status file (CIASTATS DD) is an optional output data set that records the results of STATUS console commands processed by the CIA real-time component. The CIA real-time journal file (CIAJRNL DD) is an optional output data set that records messages about internal warnings and failures that occur during the processing of an update event.

CA ACF2: CAI.CAX1JCL0

CA Top Secret: CAI.CAK0JCL0

Define the CIA Real-time Component Procedure

CIARTUPD

This is the CIA real-time component started task procedure, which is copied from the CA ACF2 or CA Top Secret installation data set to a procedure library in each z/OS system where the CIA real-time component is executed.

CA ACF2: CAI.CAX1PROC

CA Top Secret: CAI.CAK0JCL0

Implementing CA Compliance Manager for CA Chorus for Security and Compliance Management

The following jobs address the requirements for implementing CA Compliance Manager for CA Chorus for Security and Compliance Management.

Configure CA LDAP Server and CA Compliance Manager

CDT9PCHR

Creates and initializes the CA Compliance Manager policy file, which holds the policy statements and policy sets that control component processing for CA Compliance Manager.

CA LDAP Server: *your_ldap_hlq*.CDT9JCL

slapd.conf

The configuration file for CA LDAP Server, which contains the appropriate policy file and DB2 table names, including suffix (company name and country code), DB location, DB user, and DB password. Note: If using a PassTicket to connect to DB2, omit the DB password and instead specify the DB2 application ID.

Default location of file: /usr/lpp/caldapr151

CDT9PBAC

Creates the backup policy file, which holds a backup copy of the policy statements and policy sets that control component processing for CA Compliance Manager.

CA LDAP Server: *your_ldap_hlq.*CDT9JCL

CDT9PRES

Restores the CA Compliance Manager policy file, which holds the policy statements and policy sets that control component processing for CA Compliance Manager.

CA LDAP Server: *yoCur.ldap.hlq*.CDT9JCL

Create the CA Datacom/AD MUF for CA Compliance Manager

AXCUS00

Creates the your_datacom_hlq.INSTJCL data set and copies members so they can be modified by the site. It builds, populates, and mass-edits the installation JCL data set.

CA Datacom/AD: *your_datacom_hlq*.CAAXSAMP

AXCUS01

This job includes all customization for the CA Compliance Manager CA Datacom/AD MUF.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

AXNEW01

Allocates and populates data sets that the CA Compliance Manager CA Datacom/AD MUF needs.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

AXRIM01

Installs the PC CALLS.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

AXAPFADD

Provides a CA SYSVIEW example to dynamically add libraries to be APF listed.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

AD14STRT

This is the job that creates the started task procedure that starts the test instance of the CA Compliance Manager CA Datacom/AD MUF.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

AXIVP01

This is a sample install verification job.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

AD14STOP

Stops the test instance of the CA Compliance Manager CA Datacom/AD MUF.

CA Datacom/AD: *your_datacom_hlq*.INSTJCL

Delete the CA Compliance Manager Repositories (If Required)

CMGRIDCD

This job deletes existing CA Compliance Manager CA Datacom/AD repositories, if required.

CA Compliance Manager: CAI.CEIQJCL0

Define CA Compliance Manager Repositories for CA Datacom/AD

CMGRIDCM

This job defines the database, tables, and applications in a CA Datacom/AD environment for the following CA Compliance Manager components:

- Warehouse
- Data Mart
- Monitor

CA Compliance Manager: CAI.CEIQJCL0

Define the CA Compliance Manager Repositories for DB2

CMGRIDB2

Defines the DB2 repositories and native DB2 security for the following CA Compliance Manager components:

- Warehouse
- Data Mart
- Monitor

CA Compliance Manager: CAI.CEIQJCL0

Allocate the CA Compliance Manager Component Output Data Sets

CMGRIALC

Allocates the status (CMGRSTAT DD) and journal (CMGRJRNL DD) output data sets for the following CA Compliance Manager components:

- Router
- Alert
- Logger
- Warehouse
- Monitor

CA Compliance Manager: CAI.CEIQJCL0

Define a DASD-Only Logstream

CMGRLDEF

Defines a DASD-only system logstream using the IBM Utility, IXCMIAPU.

CA Compliance Manager: CAI.CEIQJCL0

Define a CF-Based Logstream

CMGRLDEF

Defines a Coupling Facility (CF)-based system logstream using the IBM Utility, IXCMIAPU.

CA Compliance Manager: CAI.CEIQJCL0

Start the CA Compliance Manager Components (Manually)

CMGRRTR

Starts the CA Compliance Manager Router component (required).

CA Compliance Manager: CAI.CEIQPROC

CMGRLOGR

Starts the CA Compliance Manager Logger component.

CA Compliance Manager: CAI.CEIQPROC

CMGRWHSE

Starts the CA Compliance Manager Warehouse component.

CA Compliance Manager: CAI.CEIQPROC

CMGRMON

Starts the CA Compliance Manager Monitor component.

CA Compliance Manager: CAI.CEIQPROC

CMGRALRT

Starts the CA Compliance Manager Alert component.

CA Compliance Manager: CAI.CEIQPROC

Allocate the Data Mart Output Data Sets

CMGRDALC

This job allocates the UNLOAD DD, STATREPT, and ERRREPT output data sets for the Data Mart.

CA Compliance Manager: CAI.CEIQJCL0

Unload Data from the Logstream Using the Data Mart

CMGRDUNL

Executes the Data Mart, which unloads selected security event information from the system Logger logstream into the UNLOAD DD data set.

CA Compliance Manager: CAI.CEIQJCL0

Execute the Data Mart CA Datacom/AD Conversion Utility

CMGRDLDC

Converts the UNLOAD DD data set information, which is in DB2 load format, into CA Datacom/AD load format and loads the information into the CA Datacom/AD Data Mart repository.

CA Compliance Manager: CAI.CEIQJCL0

Load the DB2 Data Mart Repository

CMGRDAL00

This job executes the DB2 Load Utility to load the security information from an UNLOAD DD data set into the DB2 Data Mart repository in the target DB2 subsystem. It executes a series of steps to load and replace the entire DB2 Data Mart repository.

CA Compliance Manager: CAI.CEIQJCL0

Load Additional Data into an Existing DB2 Data Mart Repository

CMGRDA00

This job executes a series of steps to load additional security information into an existing DB2 Data Mart repository in the target DB2 subsystem without replacing any data.

CA Compliance Manager: CAI.CEIQJCL0

Appendix B: STC Reference

This section contains the following topics:

STC Reference and Start/Stop Order

The table that follows details all of the Started tasks (STCs) that are required for a CA Chorus for Security and Compliance Management installation. These tasks should be started in the order described by the table, beginning with group 1. When stopping tasks, work in reverse order from group 7 to group 1. All required tasks in a group must be completely initialized or stopped before proceeding to the next group.

Note: The STC names below are the default values from the Unified Install process. The tasks in group 6 and group 7 are from the customization process for your CA Chorus deployment. If you changed any of these STC names away from the default, use those changed (non-default) names when you start and stop the tasks.

Group #	STC Name	Description	Purpose
Group 1	CIA4MUF	Multi-User Facility for CIA Database Not used in DB2 configurations.	Required for CIA database utilization.
	CMGR4MUF	Multi-User Facility for CA Compliance Manager Database Not used in DB2 configurations.	Required for CA Compliance Manager utilization.
Group 2	CIA4SRV	Server for CIA Database and MUF Not used in DB2 configurations.	Required for CA Chorus to communicate with the CIA database.
	CMGR4SRV	Server for CA Compliance Manager Database and MUF Not used in DB2 configurations.	Required for CA Chorus to communicate with the CA Compliance Manager database.

Group #	STC Name	Description	Purpose
Group 3	LDAP4SRV	Server for CA LDAP	Required for CA Chorus to communicate with the various CIA and CA Compliance Manager components.
	DSI4SRV	Server for CA DSI	Required for CA Chorus to communicate with the various CIA and CA Compliance Manager components.
Group 4	CIA4RT	CIA Real-Time Updates	Required component for updating CIA database in real time.
	CMGR4RT	CA Compliance Manager Router	Required component that routes various security events to the CA Compliance Manager components in Group 5.
Group 5	CMGR4LG	CA Compliance Manager Logger	Optional component that writes the events received from the Router to the CA Compliance Manager Logstream.
	CMGR4WH	CA Compliance Manager Warehouse	Optional component that records the security events received from the Router to the Warehouse repository in real time.
	CMGR4CM	CA Compliance Manager Change Monitor	Optional component that monitors, detects, and collects information about changes to the ESM configuration options, PDS/PDSE members, and z/OS configuration controls.
	CMGR4AL	CA Compliance Manager Alerts	Optional component that detects security events and sends external alerts when they occur.
Group 6	CHORNTSF	Time Series Facility Server	Required for communication with Time Series Facility (TSF) database.
	CHORTSFB	Time Series Facility Bridge	Required for communication between Security product (CA ACF2, CA Top Secret, RACF) and the TSF database.

Group #	STC Name	Description	Purpose
	CHORJBOS	CA Chorus Application Server (formerly named Jboss Server)	Required component that runs the CA Chorus GUI and communicates with the other components.
Group 7	CHORTSFR	Time Series Facility Relay	Optional component. Only use if you need to collect Time Series data from a system other than the system CA Chorus Platform is running on.