CA Top Secret® for z/OS

Compliance Information Analysis Guide

r15

Fourth Edition

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

CA Technologies Product References

This document references the following CA Technologies products:

- CA ACF2™ for z/OS (CA ACF2)
- CA Common Services® (CA Common Services)
- CA Chorus
- CA Chorus for Security and Compliance Management
- CA Datacom®/AD
- CA Datacom®/DB
- CA Distributed Security Integration Server for z/OS (CA DSI Server)
- CA Top Secret® for z/OS (CA Top Secret)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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 last release of this documentation:

- Implement User-Defined Fields in the CIA Repository (see page 20)—Removed obsolete information and consolidated this content into one procedure.
- Sample Unload Utility Report Output (see page 30)—Updated sample output to reflect information for user fields being processed and to reflect information for records CMXREF, DCOCLASS, DCOREC, FACSYSX, FILTER, RESXREF, UDFCHAR, USERLNTE, and USERNDS.
- GLOBALID Control Statement—Specify the Global ID (see page 36)—Updated this control statement description to clarify how the unload utility determines the default global ID.
- USERFIELD—Add User-Defined Fields to the UNLOAD Data Set (see page 37)—Updated this control statement description to reflect current functionality and parameters.
- CIA Real-Time Control Options (see page 149)—Removed obsolete options CIAGBLEXIT and CIAGBLFIELD.
- Moved the "Data Dictionary" and "Data Model" chapters to the new *CA Top Secret Data Model Guide.*

Contents

Chapter 1: Introduction 11

Chapter 2: Configuring the CIA Repository 13

Chapter 3: Unloading the Security Information 25

Chapter 4: Load the Security Information 43

Chapter 5: Compliance Information Analysis Reports 55

Chapter 6: Examples of Ad-Hoc SQL Queries 99

Chapter 7: CIA Service Functions 103

Chapter 1: Introduction

Use the Compliance Information Analysis (CIA) feature to replicate compliance security information from the mainframe security database into a CIA relational data repository. The compliance information replicated in the repository is account (user) information and policy (rules or permissions) information. Other types of information contained in the security databases are not included in the data repository.

This section contains the following topics:

Audience

This guide is intended for the following administrators:

- Security administrators who run the CIA unload and load utilities, and run and analyze reports
- Systems programmers who install and configure the CIA feature
- Auditors who analyze the CIA reports for auditing and compliance purposes

Benefits

After compliance security information is replicated into a CIA relational repository, the data can be used to do the following:

- Service a set of compliance reports, which are distributed with the security product. These distributed reports are modeled to report on role-based security authorizations. Reports can help sites and auditors more easily analyze and report on compliance-related issues based on the roles defined within a site.
- Service ad-hoc SQL queries. You enhance query performance by issuing ad-hoc SQL queries against compliance security information in the CIA relational repository, rather than directly against the mainframe security database.
- Service customized security applications and reports. Every site has specific and unique needs, which require the ability to extract and use data in different ways. Sites can determine how to use the compliance security information in the repository to create their own applications.

Command Notation

This guide uses the following command notation.

Enter the following exactly as they appear in command descriptions:

UPPERCASE

Identifies commands, keywords, and keyword values that must be coded exactly as shown.

MIXed Cases

Identifies command abbreviations. The uppercase letters are the minimum abbreviation; lowercase letters are optional.

lowercase italics

Indicates that you must supply a substitution (a user-supplied value).

symbols

All symbols (such as equal signs) must be coded exactly as shown. The following symbols clarify command syntax; do not type these symbols as they appear:

[ ]

Identifies optional keywords or parameters.

{ }

Requires choosing one of the keywords or parameters listed.

underline

Shows default values that you do not need to specify.

|

Separates alternative keywords or parameters, choose one.

…

Indicates the preceding items or group of items can be repeated more than once.

Chapter 2: Configuring the CIA Repository

This chapter steps you through the tasks required for configuring the CIA feature. Perform these tasks only *once*, in the order specified.

This section contains the following topics:

The CIA Repository

The security information you load into the CIA repository is used for a set of compliance reports that are distributed with your security product. You can use the information in the repository to run ad-hoc SQL queries, because the query is not possible with the security product command, or the same query executed against the mainframe security databases would affect the performance of your security product.

You can also develop customized security applications and reports that use the security information in the CIA repository.

CA Chorus for Security and Compliance Management leverages the information in the CIA repository to provide user (account) and security policy information for the CA Chorus security role.

The following concepts are important to understanding the usefulness of the CIA repository:

- The mainframe security products use the security information in the mainframe security database, not in the CIA repository. The information in the repository is replicated from the mainframe security database, and is only intended to be read in servicing reports, CIA queries, customized applications, and CA Chorus. If you modify information in the CIA repository, it does not affect processing in the security product. However, the CIA repository then no longer accurately reflects the information in the mainframe security database.

- Unless you have CA Chorus and are using the CIA real-time feature, the information in the CIA repository is only as accurate as the last time it was replicated from the mainframe security database. Information in the repository is not updated in real time when information in the security database is changed. If you need current information in a set of reports or SQL queries, arrange to have the current security information replicated to the repository before running the reports or queries.
- If you have CA Chorus for Security and Compliance Management, you can use the CIA real-time feature to maintain the CIA repository such that it is an accurate reflection of current information in the security product databases. For more information see CIA Real-Time Processing for CA Chorus (see page 131).

How to Choose the CIA Repository

The CIA security repository contains information about your mainframe users and the mainframe security policy. This information can reside in a CA Datacom/AD Multi-User Facility (MUF), a CA Datacom/DB MUF, or in a DB2 subsystem.

The first step in defining the security repository is to decide where the CIA repository resides. CA Datacom/AD is available as a component of CA Common Services on support.ca.com and can be used to hold the CIA repository. If you are licensed for CA Datacom/DB or IBM DB2 on the LPAR that contains the CIA repository, these alternatives can be used to hold the CIA repository.

Use the following criteria to choose a secure location for your CIA repository:

- Limit access to the security repository to people who already are able to list user and policy information directly from the mainframe security database. This restriction factors into the decision on which CA Datacom MUF or DB2 subsystem is to contain the security repository.
- Do not establish the security repository in a CA Datacom MUF or DB2 subsystem that functions as an application server. These systems traditionally have system administrators that can access the information in any database. The administrators would also be able to access the information in the security repository.
- Generate a CA Datacom Multi-User Facility (MUF) or DB2 subsystem that holds only the security repository. Give access to the CA Datacom MUF or DB2 subsystem only to people with access to the security information. This restriction eliminates any possibility of users with application access being able to access the security information.
- Verify that only people with the proper authority can access the security repository. Verify authorities regardless of whether you generate a stand-alone CIA repository or choose an existing CA Datacom MUF or DB2 subsystem.

Software Prerequisites

Before you perform any implementation tasks for CIA, verify that you have installed all the required software.

Your software must meet the following minimum requirements:

- Any supported release of CA Top Secret for z/OS
- If you are using CA Datacom for the CIA security repository:
  - CA Datacom®/AD Version 14 (from CA Common Services) or CA Datacom®/DB Version 14
- If you are accessing the CIA security repository in CA Datacom from the CA Chorus for Security and Compliance Management role:
  - CA Datacom Server Version 14
- If you are using DB2 for the CIA security repository:
  - Any supported release of IBM DB2 for z/OS
  - Workload Manager (WLM)
  - Resource Recovery Attach Facility (RRSAF)

Installing the CA Common Services Easytrieve Component

The CA Easytrieve component of CA Common Services is required only for the compliance reports. Before running the compliance reports distributed with the CIA feature, install the CA Easytrieve component of CA Common Services.

Note: For complete information about installing this Common Services component, see *CA Common Services for z/OS Installation Guide*.

For more information, see Software Requirements.

Install the CA-PAN/SQL Interface

CA Pan/SQL is required only for the compliance reports.

The CA Common Services CA Easytrieve component calls CA Pan/SQL when the reports are run. Before running the compliance reports distributed with the CIA feature, install the CA Pan/SQL interface, which has been supplied on a separate tape from your security product. For complete information about how to install CA Pan/SQL, see *CA Pan/SQL Getting Started*.

Update member OMSMCMD2 in the Pan/SQL CAIMAC library, and set MAXCUR=40.

Note: If you have CA Pan/SQL already installed, and MAXCUR is set to at least 40, then you can skip this step.

To set MAXCUR=40

For new installs:

1. Verify that member OMSMCMD2 has been updated to say MAXCUR=40.
2. Run job IJ3STGE1 from the CA Pan/SQL INSTALL.JCL library.

   Note: For additional information about customizing CA Pan/SQL, see *CA Pan/SQL Getting Started.*

If CA Pan/SQL is already installed:

1. Update member OMSMCMD2 to say MAXCUR=40.
2. Run job IJ3STGE1 from the CA Pan/SQL INSTALL.JCL library.

   Note: For DB2 users, DB2 SYSADM authority is required to run IJ3STGE1.
3. Run job CB2ACMDL from the CA Pan/SQL INSTALL.JCL library.

For more information, see Software Requirements.

Implement the CIA Repository in CA Datacom

Perform the following steps to implement the CIA repository in CA Datacom.

Install the CA Datacom/AD Component

If you are not licensed for CA Datacom/DB or IBM DB2 on the LPAR on which the CIA repository resides, or if you wish to use CA Datacom/AD to hold the CIA security repository, install the CA Datacom/AD component.

CA Datacom/AD is a limited version of the CA Datacom/DB DBMS software, available as a component of CA Common Services.

If you are implementing the CIA repository as part of an installation of the CA Chorus for Security and Compliance Management role, the CA Datacom/AD component may already be installed.

Note: For complete information about installing the CA Datacom/AD component, see the CA Common Services for z/OS *Installation Guide* and the CA Datacom/AD *Installation Guide for z/OS.*

Create the CA Datacom MUF

After CA Datacom is installed, create and deploy the CA Datacom Multi-User Facility (MUF) that holds the CIA repository.

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

After creating and deploying the CA Datacom MUF, copy the CIAMUF sample procedure from the CAI.CAKOJCL0 installation data set to a procedure library. Edit and modify the CIAMUF procedure to conform to your installation standards.

Note: The CIAMUF procedure references Datacom initialization parameters that are distributed in the CAI.CAKOOOPTN 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 Security Definitions for the CA Datacom MUF

Before bringing up the CA Datacom MUF that holds the CIA repository, create the security definitions for the MUF and the CIA repository and the authorizations for the users who will access the CIA repository.

Follow these steps:

1. Edit the CIASECC job in 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.

Start the CA Datacom MUF

The CA Datacom MUF should now be started. The MUF must be executing before the CIA repository can be defined.

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

Link the CIA Functions with CA Datacom

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

Follow these steps:

1. Edit the CIALINKC 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 CIALINKC job.

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

Define the CIA Repository to CA Datacom

Before the CIA application and repository can be defined in CA Datacom, the service function modules linked in the prior step must be available in the CA Datacom MUF. The CA Datacom MUF must be executing, and the target data set of the link authorized and available in the STEPLIB concatenation of the CA Datacom MUF.

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

- Allocate the data sets to hold the CIA repository database.
- Define the CIA database to the CA Datacom 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 to define the CIA repository.

1. Edit the CIADCOM job in 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.

Implement CA Datacom Server

If you are implementing the CIA repository as part of an installation of the CA Chorus for Security and Compliance Management role, you must implement a CA Datacom/AD Server on the same LPAR as the CA Datacom/AD MUF containing the CIA repository. CA Chorus requires the CA Datacom/AD Server to access the CIA repository in the CA Datacom/AD MUF.

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

After deploying the CA Datacom/AD Server for the CIA repository, ensure that the initialization parameters for the CA Datacom/AD Server have the following values:

```
SERVERNAME=CIAx_SYSy or CMGRx_SYSy
APPLID=CIAx_SYSy or CMGRx_SYSy
PLANNAME=$MBH
AUTHID=SYSUSR
PROTOCOL=BOTH
TCPIP_HOST=LPARNAME
DBUSERS=900
TIMEOUT=6
TIMEOUTWAIT=10
CHRUSEXT=CHRCXT10
```

Implement the CIA Repository in DB2

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

1. Create the DB2 subsystem
2. Set up Workload Manager (WLM) and Resource Recovery Attach Facility (RRSAF)
3. Start the DB2 subsystem
4. Define the CIA repository in DB2

Create the DB2 Subsystem

Create and deploy the DB2 subsystem that holds the CIA repository.

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

Set Up Workload Manager and Resource Recovery Attach Facility

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. 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. We recommend that you set up a separate WLM environment for the CIA user-defined functions and stored procedure.

Start the DB2 Subsystem

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

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

Implement User-Defined Fields in the CIA Repository

If your site has defined its own user fields on the ACID, you can include this information in the CIA repository.

Note: This implementation must occur *after* you have installed required software but *before* performing additional CIA implementation tasks. For information about how to define user fields to CA Top Secret by using the Field Descriptor Table (FDT), see the *CA Top Secret User Guide.*

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 UDFCHAR table records containing the fields).

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.

Follow these steps:

1. Edit the CIAUNLD job in CAI.CAK0JCL0 by customizing the USERFIELD control statement to specify one of the following values:
   - ***ALL*** (to add all user-defined fields)
   - ***NONE*** (to *omit* user-defined fields)
   - *field_name* (to add a specific external user-defined field name to the repository)

     Note: You can specify multiple field names to add. If no CA Top Secret FDT entry matches the field name that is specified in the USERFIELD control statement, the unload utility terminates.
2. Submit the CIAUNLD job.

   Data customization is complete in the CIAUNLD job, and the product loads the user-defined fields into the repository.

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 *
INPUT(DATASETS)
/*
```

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*)
/*
```

More information:

USERFIELD—Add User-Defined Fields to the UNLOAD Data Set (see page 37)

Define the CIA Repository to DB2

After you have created and started the DB2 subsystem to hold the CIA repository, you can define the CIA application and repository to DB2.

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 CIALINK job in CAI.CAK0JCL0.

   Modify it to conform to your installation standards, and direct it to the target DB2 subsystem.

2. Submit the job.

   The job runs and completes.

3. Verify the output of the CIALINK job.

   The CIA modules are linked.

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.
- 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, and CIABIND) that were run with previous CIA releases.

Prior to submission of this job, you must ensure that the DB2 subsystem into which the CIA repository will be installed is running.

Follow these steps:

1. Edit the CIADB2 job in CAI.CAX1JCL0.

   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.

   If you decide to include user defined fields in the CIA repository, modify the DDL statements within the CIADDL step before running the CIADB2 job.

2. Submit the job.

   The job runs and completes.

3. Verify the output of the CIADB2 job.

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

CA Chorus and CIA Real-Time Processing

CA Chorus for Security and Compliance Management leverages the user (account) and security policy information in the CIA repository.

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

If you are implementing the CIA repository as part of an installation of the CA Chorus for Security and Compliance Management role, you must perform the CIA unload and load processing as part of an implementation of CIA real-time processing.

More information:

How CIA Real-Time Processing Works (see page 133)

Chapter 3: Unloading the Security Information

This section contains the following topics:

How Unloading the Security Information Works

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) 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 for the CIA repository.

For more information, see Load the Security Information (see page 43).

How to Unload the Security Information

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.

Perform the following tasks to unload the security information from the security database:

1. Run TSSFAR utility.
2. Run the CFILE job.
3. Estimate storage requirements for the UNLOAD data set.
4. Allocate the UNLOAD data set.
5. Check your authorization to run the unload utility.
6. Run the UNLOAD utility.

7. Specify user-defined fields to be unloaded.
8. 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.

Estimate Storage Requirements

The following explains how to estimate the amount of space (in cylinders) to allocate the UNLOAD utility data set.

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.

Worksheet

The following worksheet has been provided to help you 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)

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)

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 the storage requirements have been calculated for the UNLOAD data set, the data set must be allocated.

To allocate the unload data set

1. Edit the CIAALLOC job in CAI.CAK0JCL0. Change the job to include the necessary space allocation and 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.

Check Authorization to Run the Unload Utility

Verify that you have authorization 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.

Run the 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 exist to control the processing of the unload utility. These statements can be specified as input to the SYSIN input data set.

To run the unload utility

1. Edit the CIAUNLD job in CAI.CAK0JCL0.

   Specify the unload data set allocated earlier and any control statements that you require to conform to the standards of your site.

2. Submit the job.

3. Check the output of the CIAUNLD job.

   Verify that the utility completed successfully. If the CIAUNLD job fails for any reason, you must rerun the job until it successfully completes; otherwise the UNLOAD data set cannot be properly loaded to the relational database and enhanced compliance reporting capabilities will not be available.

For more information, see JCL Requirements and Control Statements (see page 34).

More Information:

Control Statements (see page 34)

JCL Requirements

The following is an example of the JCL required to execute the CIAUNLD unload utility:

```
//jobname JOB …
//CIAUNLD  EXEC PGM=TSSCIALD
//UNLOAD   DD  DSN=unload.data.set,DISP=OLD
//CFILE    DD  DSN=cfile.data.set,DISP=SHR
//PRECFILE DD  DSN=precfile.data.set,DISP=SHR
//REPORT   DD  SYSOUT=*
//SYSIN    DD  *
control statements
//
```

Check Output from Unload

The unload utility writes statistical information and any error messages to a report file. The report includes the following information:

- A detailed summary of the type and number of records processed from the security file.
- A detailed summary of the type and numbers of records created in the unload utility data set.
- Error messages (processing terminates if any error messages are issued).
- Warning messages indicate that unexpected data was encountered. This data was not written to the UNLOAD dataset and the message contains the line number in the CFILE dataset where the unexpected data was found. The UNLOAD dataset can be used to load the repository if warning messages are issued. Review warning messages and take appropriate action. For descriptions of CIA messages, see the *Messages Reference Guide*.

Return Codes

The unload utility returns the following codes:

0

Unload process was successful

8

The output report file did not open

12

Unload process failed (a diagnostic message was issued)

Sample Unload Utility Report Output

Following are examples of the unload utility output report file. All examples completed successfully.

```
                  CA Top Secret Unload Utility Report
                          DATE 2007-02-01 TIME 10:43

Processing Exception Report

TSSC100I - SYSID (XE31    ) WAS SET FROM PARAMETER FILE.
TSSC050W - CFILE WAS NOT RUN BY A MSCA IT MAY BE AN INCOMPLETE FILE
TSSC051W - BAD RECORD TYPE (USERTSO ) FOR ACID (ACF2D   ) TYPE D
TSSC051W - BAD RECORD TYPE (USERCICS) FOR ACID (SMFDEPT3) TYPE D
TSSC016W - NO RESOURCE OWNERSHIP WAS FOUND FOR THIS PERMIT REC #      485,976
TSSC016W - NO RESOURCE OWNERSHIP WAS FOUND FOR THIS PERMIT REC #      507,289
```

```
                                                               PAGE    1

                 CA Top Secret Unload Utility Report
                         DATE 2007-02-01 TIME 10:43
                          Processing SYSID  XE31

Processing Unload Statistics

                                 Lines processed for cfile report       894,108
User Acid Information

Records processed for User ACIDS                  22,937
User fields being processed                           24
```

```
USERINFO records generated                                22,937
  USERTSS  records generated                              22,937
  IDMAP    records generated                              22,937
  LDSREC   records generated                                   0
  SMSINFO  records generated                                   7
  SMSXREF  records generated                                   7
  SRCREC   records generated                                   4
  USERCICS records generated                               5,739
  USERDCE  records generated                                   0
  USERGRP  records generated                               1,121
  USERKBLK records generated                                   0
  USERKERB records generated                                   0
  USERLANG records generated                                   1
  USERNETV records generated                                   0
  USERNODE records generated                                   7
  USERNVCL records generated                                   0
  USERNVDM records generated                                   0
  USEROMVS records generated                                 904
  USEROPER records generated                                   5
  USERSECL records generated                                   0
  USERTSO  records generated                              21,227
  USERWRKA records generated                                   9
  UDFCHAR  records generated                                  38
  USERNDS  records generated                                   1
  USERLNTE records generated                                   1
  User Administration Information

  Records processed for Acid Administration                  377
  Records processed for Data Admin                           365
  Records processed for Facility Administration              252
  Records processed for Misc. Administration                 374
  Records processed for Misc1 Administration                 361
  Records processed for Misc2 Administration                 178
  Records processed for Misc3 Administration                  34
  Records processed for Misc4 Administration                  41
  Records processed for Misc5 Administration                   0
  Records processed for Misc8 Administration                 103
  Records processed for Misc9 Administration                 155
  Records processed for Resource Administration              758
  Records processed for Role Administration                1,296
  ADMNUSER records generated                                 377
  ADMNDATA records generated                                 365
  ADMNFAC  records generated                                 252
  ADMNMISC records generated                                 374
  ADMNRES  records generated                                 655
  ADMNROLE records generated                               1,296
```

```
                                                                  PAGE     2
                     CA Top Secret Unload Utility Report
                           DATE 2007-02-01 TIME 10:43
                           Processing SYSID  XE31

Processing Unload Statistics

Permit Information
  Records processed for User Permits                56,065
  Records processed for Role Permits                52,052
  PERMXREF records generated                       108,117
  PERMFACX records generated                            96
  PERMLIBX records generated                            19
  PERMPGMX records generated                           119

Profile Information

  Records processed for Profiles                     3,685
  Records processed for Groups                           0
  ROLEXTR records generated                          3,685
  ROLEATTR records generated                         3,685
  ROLEINFO records generated                         3,686
  ROLEXREF records generated                        31,742


Facility Information

  Records processed for Facility User              106,937
  Records processed for Facility Role                  408
  FACXREF  records generated                       107,345
  FACCMND  records generated                           186
  FACLINUX records generated                             0
  FACLTIME records generated                            33
  FACSITRN records generated                            19
  FACSYSX  records generated                             1

Resource Information

  Number of resources added to table                74,126
  Records processed for Resource Owners             74,126

  RESINFO  records generated                        74,126

Scope Information

  SCPXREF  records generated                        22,814
  SCPNEXT  records generated                        20,808
  SCPPROF  records generated                         3,685
  SCPRES   records generated                        74,126
  SCPUSER  records generated                        22,469

EIM/Proxy Information

  EIMREC   records generated                             0
  PROXYREC records generated                             0

Shift Record information

  DAYINFO  records generated                             0
  DAYREC   records generated                             0
  TIMEINFO records generated                             0
  TIMEREC  records generated                             0
```

```
Dataclass Information

  DCOCLASS records generated                             4
  DCOREC   records generated                             4
```

```
                                                               PAGE    3

                   CA Top Secret Unload Utility Report
                           DATE 2007-02-01 TIME 10:43
                           Processing SYSID  XE31

Processing Unload Statistics

System Information

  SYSINFO  records generated                             1
  FILTER   records generated                             1
  RESXREF  records generated                           189
  CMXREF   records generated                             1
```

Control Statements

The unload utility supports several control statements that can be used to modify processing. These control statements can be used to:

- Specify a different SYSID to be used in the repository
- Specify a field or exit to be used to populate the GLOBALID field
- Specify user-defined fields to be included in the repository
- Filter the users and resources to be included in the repository

SYSID Control Statement

SYSID Modification

By default, the unload utility puts a value corresponding to the MVS system ID in the SYSID fields in the repository. To substitute a different, more meaningful value in the SYSID field in the repository table records, use the SYSID control statement.

```
SYSID(sysidvalue)
```

SYSID

Contains a value that specifies to which system (z/OS system image) the table record information applies. All of the tables in the data repository have a SYSID field as part of the key for the table.

Limits: Only one SYSID control statement can be specified in the SYSIN file. The SYSID keyword cannot be abbreviated.

sysidvalue

(Optional) Specifies the character value substituted in the SYSID field in the repository table records.

Limits: 1 to 8 characters

LPAR Control Statement

LPAR Modifications

The CIA CMXREF table contains information about the relationship between each security file that was loaded into the CIA repository and the z/OS images or LPARs that share that security file. In a CA Chorus for Security and Compliance Management implementation, the information is used to correlate CA Compliance Manager events from each z/OS image or LPAR with the CIA user and policy information that corresponds to the event.

The CMXREF table also contains CIA real-time status connection information for CIA heartbeat events. By default, the unload utility generates a record for the CMXREF table and uses the value corresponding to the MVS system ID in the LPAR field. However, you can use the LPAR control statement to override the default value and add multiple records when multiple systems share the security file.

This control statement has the following format:

```
LPAR(lparvalue)
```

lparvalue

Specifies the character value to place in the LPAR field in the CMXREF table record that the unload utility generates.

Note: A CMXREF record is defined for each specified LPAR. If multiple systems share a security file, you must use the LPAR keyword to generate a record for each system that updates the CIA repository in real time or generates CA Compliance Manager events. The LPAR keyword cannot be abbreviated.

Limits: 1-8 characters

GLOBALID Control Statement—Specify the Global ID

A global ID connects userids from several systems to a single user. For example, an individual user can have two userids (TESTID1 and TESTID2) on system image SYSTEMT and one userid (PRODID1) on system image SYSTEMP. A global ID allows all of the userids to be associated to the individual user.

By default, the unload utility populates the GLOBALID column in the IDMAP table with a value that corresponds to the eight-character ACID that is being processed.

To substitute a different value in the GLOBALID field, use the GLOBALID control statement to specify an ACID field or an exit routine to populate the GLOBALID column.

Note: Only one GLOBALID input control statement can be specified in the SYSIN file. The GLOBALID keyword cannot be abbreviated.

This control statement has the following format:

```
GLOBALID FIELD(field_name)|EXIT(exit_name)
```

GLOBALID FIELD(*field_name*)

Specifies the external name of a field from a predefined list of fields in the userid (ACID) or specifies a user-defined field that has a length of less than 32 bytes. The unload utility uses the value of the field as the GLOBALID value. If a GLOBALID value does not exist on the userid for the specified field, the GLOBALID field is left blank and a warning message appears in the Unload report.

Note: The FIELD keyword cannot be specified with the EXIT keyword. The FIELD keyword cannot be abbreviated.

GLOBALID FIELD(*exit_name*)

Specifies the name of a user GLOBALID exit module residing in the link pack area (LPA). The unload utility calls this exit to supply a GLOBALID. The utility passes a parameter list to the exit that contains the current userid value that is being processed. The utility expects the user exit to return a valid, 1- to 32-byte GLOBALID value for that userid in the parameter list. If the exit does not return a GLOBALID value, the unload utility terminates with an error.

Note: The EXIT keyword cannot be specified with the FIELD keyword. The EXIT keyword cannot be abbreviated. For more information about using the GLOBALID exit, see the appendix GLOBALID Exit (see page 129).

USERFIELD—Add User-Defined Fields to the UNLOAD Data Set

Use the USERFIELD control statement to add user-defined fields into the UNLOAD data set so that the fields can be replicated in the CIA repository. The control statement is optional. To specify more than one unique USERFIELD(*field_name*) control statement, you must specify each control statement on a separate line in the SYSIN file. The USERFIELD keyword *cannot* be abbreviated. If no USERFIELD input control statements are specified in the CIA unload utility SYSIN file, the default is USERFIELD(*ALL*).

This control statement has the following format:

```
USERFIELD(*ALL*|*NONE*|field_name)
```

ALL

Specifies that all CA Top Secret displayable user-defined fields in the Field Descriptor Table (FDT) are added to the UNLOAD data set. This value is the default value.

Note: If USERFIELD(*ALL*) is specified, you cannot specify other USERFIELD input control statements.

NONE

Specifies that no CA Top Secret user-defined fields in the FDT are added to the UNLOAD data set. USERFIELD(*NONE*) may be specified only once in the SYSIN file.

Note: If USERFIELD(*NONE*) is specified, you cannot specify other USERFIELD input control statements.

field_name

Specifies the display name of a displayable user-defined field that you want to add to the UNLOAD data set. The entry corresponds to a valid FDT entry. This value must be between 1 and 11 characters and must be defined as displayable. USERFIELD(*field_name*) may be specified more than once, but is mutually exclusive with USERFIELD(*ALL*) or USERFIELD(*NONE*) input control statements. Duplicate USERFIELD(*field_name*) statements are not allowed.

More information:

Implement User-Defined Fields in the CIA Repository (see page 20)

INCLUDE/EXCLUDE Processing

The UNLOAD utility processes the INCLUDE and EXCLUDE control statements to allow a subset of userid, resources (or both) to be loaded. If no INCLUDE or EXCLUDE statements are specified, all users and resources are loaded into the CIA repository. The INCLUDE and EXCLUDE statements can be specified in any order.

INCLUDE/EXCLUDE Control Statements—Filter ACIDs

ACIDs of type USER, VCA, DCA, and ZCA can be excluded from the repository by using the INCLUDE and EXCLUDE statements. ACIDs of type PROFILE, GROUP, SCA, LSCA, and MSCA are included in the repository even if a matching exclude statement is specified. In addition, all resource ownership and administrative authority information are always included in the repository. ACIDs of type USER, VCA, DCA, ZCA, DEPARTMENT, DIVISION, and ZONE can be specified on an INCLUDE or EXCLUDE statement. If an ACID of another type is specified, the statement is accepted but will not affect processing.

If an organizational acid such as a department, division, or zone is specified, the INCLUDE or EXCLUDE applies to all USER, VCA, DCA, and ZCA acids belonging to that organization. Resource ownerships and PROFILE and GROUP type acids that belong are included in the repository even if the organizational acid is excluded.

If an ACID is excluded from the repository, no user information is loaded. No records are generated for the excluded ACID except for resource ownership and administrative authority information. This information is needed to correctly report on administrative scope and permissions to the owned resource for other acids.

If multiple INCLUDE and EXCLUDE statements match an ACID, the most specific statement is used. The following list is the order of most specific to least specific:

- INCLUDE/EXCLUDE ACID(*useracid*)
- INCLUDE/EXCLUDE ACIDPRFX(*useracidprefix*)
- INCLUDE/EXCLUDE ACID(*deptacid*)
- INCLUDE/EXCLUDE ACIDPRFX(*deptacidprefix*)
- INCLUDE/EXCLUDE ACID(*divacid*)
- INCLUDE/EXCLUDE ACIDPRFX(*divacidprefix*)
- INCLUDE/EXCLUDE ACID(*zoneacid*)
- INCLUDE/EXCLUDE ACIDPRFX(*zoneacidprefix*)
- INCLUDE/EXCLUDE ALLACIDS

Note: useracid and useracidprefix can be type USER, DCA, VCA, or ZCA.

If multiple INCLUDE/EXCLUDE ACIDPRFX(*acidprefix*) statements are specified for the same acid type, the longest *acidprefix* is considered more specific. If the same acid or acid prefix is specified on both an INCLUDE and an EXCLUDE statement, the INCLUDE statement is used.

INCLUDE ALLACIDS

ALL USER, DCA, VCA, and ZCA acids are loaded into the CIA repository unless a more specific EXCLUDE statement applies. INCLUDE ALLACIDS is the default and is in effect unless EXCLUDE ALLACIDS is specified.

EXCLUDE ALLACIDS

If specified, no USER, DCA, VCA, or ZCA acids will be loaded into the CIA repository except for acids and organizations specified on an INCLUDE statement.

INCLUDE ACID(*acidname*)

The specified ACID is included in the repository. If *acidname* is an organizational acid, all acids in that organization are also included unless a more specific EXCLUDE statement applies.

Limits: 1 to 8 characters. Only one acid name may be specified for each INCLUDE statement.

EXCLUDE ACID(*acidname*)

The specified ACID is excluded from the repository. If *acidname* is an organizational acid, all acids in that organization are also excluded unless a more specific INCLUDE statement applies.

Limits: 1 to 8 characters. Only one acid name can be specified for each EXCLUDE statement.

INCLUDE ACIDPRFX(acidprefix)

Any ACID that matches the specified prefix is included in the repository. If the matching ACID is an organizational acid, all acids in that organization are also included unless a more specific EXCLUDE statement applies.

Limits: 1 to 7 characters. Only one prefix may be specified for each INCLUDE statement.

EXCLUDE ACIDPRFX(*acidprefix*)

Any ACID that matches the specified prefix is excluded from the repository. If the matching ACID is an organizational acid, all acids in that organization are also excluded unless a more specific INCLUDE statement applies.

Limits: 1 to 7 characters. Only one prefix may be specified for each EXCLUDE statement.

INCLUDE/EXCLUDE Control Statements—Filter Resources

Resource classes and resource entities can be specified on INCLUDE and EXCLUDE statements to allow a subset of resource permissions to be loaded into the repository. If ACID filtering is also being used, no resource permissions are loaded for ACIDs that are being excluded from the repository. If an ACID is included in the repository, resource filtering can control which permissions are loaded.

If multiple INCLUDE and EXCLUDE statements match a resource, the most specific statement is used. The following list is the order of most specific to least specific:

- INCLUDE/EXCLUDE RESCLASS(resclass) RES(entity)
- INCLUDE/EXCLUDE RESCLASS(resclass) RESPRFX(entityprefix)
- INCLUDE/EXCLUDE RESCLASS(resclass)
- INCLUDE/EXCLUDE ALLRES

Note: Resource filtering only applies to resource permissions. All resource ownerships are always loaded into the repository.

If multiple INCLUDE/EXCLUDE RESCLASS(resclass) RESPRFX(entityprefix) statements are specified for the same resource class, the longest entityprefix is considered more specific. If the same resource class and resource entity or prefix is specified on both an INCLUDE and an EXCLUDE statement, the INCLUDE statement is used.

INCLUDE ALLRES

All resources are loaded into the CIA repository unless a more specific EXCLUDE statement applies.

Default: INCLUDE ALLRES is the default and is in effect unless an EXCLUDE ALLRES is specified.

EXCLUDE ALLRES

No resource permissions are loaded into the CIA repository except for resources specified on INCLUDE statements.

INCLUDE RESCLASS(*resclass*) RES(*entity*)

The specified resource is included in the repository. Permissions that exactly match the specified entity are included in the repository. *resclass* is the resource class name. *entity* is the resource entity.

Limits: *resclass*—1 to 8 characters, masking is not allowed. *entity*—1 to 255 characters; masking characters can be used but are not used as a mask but rather will match a masked permission.

EXCLUDE RESCLASS(*resclass*) RES(*entity*)

The specified resource is excluded from the repository. Permissions that exactly match the specified entity are excluded from the repository.

Limits: *resclass*—1 to 8 characters, masking is not allowed. *entity*—1 to 255 characters; masking characters can be used but are not used as a mask but rather will match a masked permission.

INCLUDE RESCLASS(*resclass*) RESPRFX(*entityprefix*)

All resources that match the entity prefix are included in the repository unless a more specific EXCLUDE statement applies.

Limits: *resclass*—1 to 8 characters, masking is not allowed. *entity*—1 to 255 characters; masking characters can be used but are not used as a mask but rather will match a masked permission.

EXCLUDE RESCLASS(*resclass*) RESPRFX(*entityprefix*)

All resources that match the entity prefix are excluded from the repository unless a more specific INCLUDE statement applies.

Limits: *resclass*—1 to 8 characters, masking is not allowed. *entity*—1 to 255 characters; masking characters can be used but are not used as a mask but rather will match a masked permission.

INCLUDE RESCLASS(*resclass*)

All resources in the specified resource class are included in the repository unless a more specific EXCLUDE statement applies.

Limits: 1 to 8 characters; masking is not allowed.

EXCLUDE RESCLASS(*resclass*)

All resources in the specified resource class are excluded from the repository unless a more specific INCLUDE statement applies.

Limits: 1 to 8 characters; masking is not allowed.

INCLUDE/EXCLUDE Control Statements—Filtering SYSIDs

Filtering SYSIDs

By default, the unload utility puts a value corresponding to the z/OS system ID in the FILTERSYSID parameter and this value is used to compare to SYSIDs that are found on permits and facilities. If the *sysid* and the *filtersysid* values match, processing of that record continues. If the *sysid* and *filtersysid* values do not match, that record is ignored and a message is written out to the exception report. To override the default value, specify the desired value with the FILTERSYSID control statement.

Note: Only one FILTERSYSID control statement can be specified in the SYSIN file. The FILTERSYSID keyword cannot be abbreviated.

```
FILTERSYSID(filtersysid_value)
```

filtersysid_value

(Optional) Specifies the character value substituted in the FILTERSYSID parameter to compare to *sysid* in the permit and facility records.

Limits: 1 to 8 characters

Chapter 4: Load the Security Information

After the CIA repository has been defined to CA Datacom 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 DBUTLTY program or the IBM DB2 LOAD utility is used to insert the security information into the CIA repository.

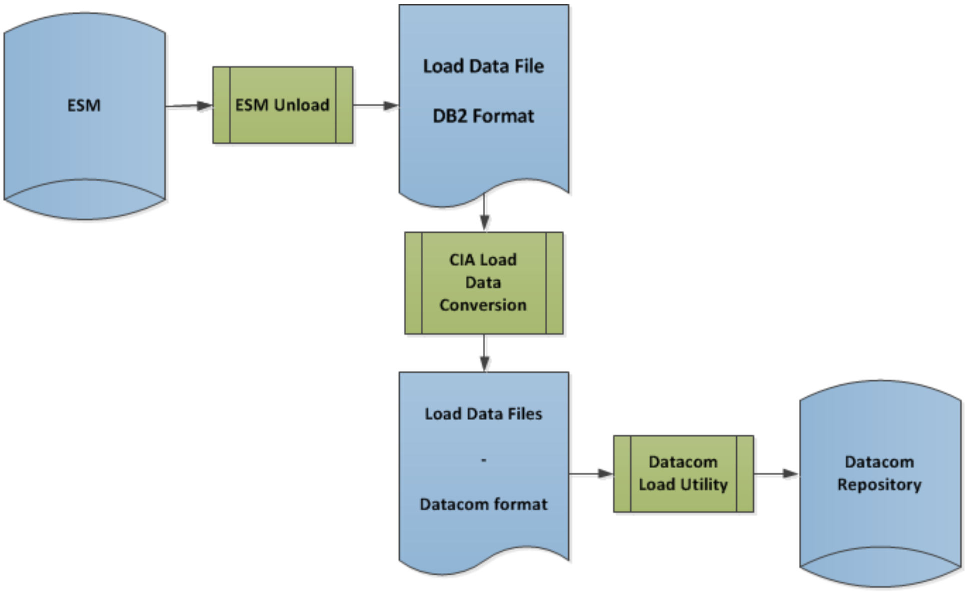
This section contains the following topics:

The Load Process for CA Datacom

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

Estimate the amount of space that is required for each CA Datacom/AD unload format data set populated by the conversion utility. Because 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.

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)

Follow these steps:

1. After running the CIAUNLD CIA unload utility, review the output Statistical Report to find the maximum count of a CIA table record type generated in the CIA UNLOAD DD data set.
2. Multiply the maximum count of a CIA table record type generated 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.

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

Load the Security Information in CA Datacom

After the CIA application and repository has been defined to CA Datacom and the security information has been unloaded with the CIAUNLD job, the CIALOADC job converts the unloaded security information from DB2 load format into CA Datacom load format and separates the converted records into individual data sets by table as required by the CA Datacom load process. It then executes the CA Datacom 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-format load data sets.
- CONVERT. Executes the CIADCCNV conversion utility to convert the unload data set created by the CIAUNLD job into the appropriate CA Datacom load format data sets.
- CLEARDB. Deletes any information currently in the CIA repository tables.
- LOAD. Executes the CA Datacom 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 CELARDB step from the job before execution.

Follow these steps:

1. Estimate the storage requirements for each of the CA Datacom UNLOAD data sets. Adjust the space allocations within the CONVERT step of the CIALOADC job as appropriate. For more information, see Estimate the Storage Requirements.
2. Edit the CIALOADC job in 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.

3. Submit the job.

   The job executes and completes

4. Verify the output of the CIALOADC.

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

The CA Datacom CIA load conversion utility, CIADCCNV, writes statistical information and any error messages to a report file. The report includes the following information:

- Any error messages during initialization or conversion processing of input UNLOAD records.
- A detailed count of the type of records converted in the load data conversion utility data sets.

Return Codes for CONVERT Step

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.

CIA Load Data Conversion Utility Inputs and Outputs

The following data sets are the input and output data sets for the CIADCCNV conversion program, executed in the CONVERT step of the CIALOADC job.

REPORT DD

Specifies a report output file. The CIA load data conversion utility writes statistical information and any error messages to this file. DCB characteristics are DSORG=PS, RECFM=FBA, LRECL=137.

UNLOAD DD

Specifies the UNLOAD data set created by CIA batch unload utility. This data set contains the security information in a DB2 load format that is input to the CIA load data conversion utility. DCB characteristics are DSORG=PS, RECFM=VB, LRECL=3157.

ADMNDATA DD

Specifies the output file for the ADMNDATA type data record in CA Datacom load format for the CIA repository.

ADMNFAC DD

Specifies the output file for the ADMNFAC type data record in CA Datacom load format for the CIA repository.

ADMNMISC DD

Specifies the output file for the ADMNMISC type data record in CA Datacom load format for the CIA repository.

ADMNRES DD

Specifies the output file for the ADMNRES type data record in CA Datacom load format for the CIA repository.

ADMNUSER DD

Specifies the output file for the ADMNUSER type data record in CA Datacom load format for the CIA repository.

CMXREF DD

Specifies the output file for the CMXREF type data record in CA Datacom load format for the CIA repository.

DATEINFO DD

Specifies the output file for the DATEINFO type data record in CA Datacom load format for the CIA repository.

DAYREC DD

Specifies the output file for the DAYREC type data record in CA Datacom load format for the CIA repository.

DCOCLASS DD

Specifies the output file for the DCOCLASS type data record in CA Datacom load format for the CIA repository.

DCOREC DD

Specifies the output file for the DCOREC type data record in CA Datacom load format for the CIA repository.

EIMREC DD

Specifies the output file for the EIMREC type data record in CA Datacom load format for the CIA repository.

FACCMND DD

Specifies the output file for the FACCMND type data record in CA Datacom load format for the CIA repository.

FACLINUX DD

Specifies the output file for the FACLINUX type data record in CA Datacom load format for the CIA repository.

FACLNXG DD

Specifies the output file for the FACLNXG type data record in CA Datacom load format for the CIA repository.

FACLTIME DD

Specifies the output file for the FACLTIME type data record in CA Datacom load format for the CIA repository.

FACSITRN DD

Specifies the output file for the FACSITRN type data record in CA Datacom load format for the CIA repository.

FACSYSX DD

Specifies the output file for the FACSYSX type data record in CA Datacom load format for the CIA repository.

FACXREF DD

Specifies the output file for the FACXREF type data record in CA Datacom load format for the CIA repository.

FILTER DD

Specifies the output file for the FILTER type data record in CA Datacom load format for the CIA repository.

GRPINFO DD

Specifies the output file for the GRPINFO type data record in CA Datacom load format for the CIA repository.

IDMAP DD

Specifies the output file for the IDMAP type data record in CA Datacom load format for the CIA repository.

LDSREC DD

Specifies the output file for the LDSREC type data record in CA Datacom load format for the CIA repository.

ORGINFO DD

Specifies the output file for the ORGINFO type data record in CA Datacom load format for the CIA repository

PERMCOLX DD

Specifies the output file for the PERMCOLX type data record in CA Datacom load format for the CIA repository.

PERMFACX DD

Specifies the output file for the PERMFACX type data record in CA Datacom load format for the CIA repository.

PERMLIBX DD

Specifies the output file for the PERMLIBX type data record in CA Datacom load format for the CIA repository.

PERMPGMX DD

Specifies the output file for the PERPGMX type data record in CA Datacom load format for the CIA repository.

PERMSYSX DD

Specifies the output file for the PERMSYSX type data record in CA Datacom load format for the CIA repository.

PERMXREF DD

Specifies the output file for the PERMXREF type data record in CA Datacom load format for the CIA repository.

PROXYREC DD

Specifies the output file for the PROXYREC type data record in CA Datacom load format for the CIA repository.

RESINFO DD

Specifies the output file for the RESINFO type data record in CA Datacom load format for the CIA repository.

RESXREF DD

Specifies the output file for the RESXREF type data record in CA Datacom load format for the CIA repository.

ROLEATTR DD

Specifies the output file for the ROLEATTR type data record in CA Datacom load format for the CIA repository.

ROLEEXTR DD

Specifies the output file for the ROLEEXTR type data record in CA Datacom load format for the CIA repository.

ROLEINFO DD

Specifies the output file for the ROLEINFO type data record in CA Datacom load format for the CIA repository.

ROLEREC DD

Specifies the output file for the ROLEREC type data record in CA Datacom load format for the CIA repository.

ROLEXREF DD

Specifies the output file for the ROLEXREF type data record in CA Datacom load format for the CIA repository.

SCPGRP DD

Specifies the output file for the SCPGRP type data record in CA Datacom load format for the CIA repository.

SCPINF DD

Specifies the output file for the SCPINF type data record in CA Datacom load format for the CIA repository.

SCPNEXT DD

Specifies the output file for the SCPNEXT type data record in CA Datacom load format for the CIA repository.

SCPPROF DD

Specifies the output file for the SCPPROF type data record in CA Datacom load format for the CIA repository.

SCPRES DD

Specifies the output file for the SCPRES type data record in CA Datacom load format for the CIA repository.

SCPUID DD

Specifies the output file for the SCPUID type data record in CA Datacom load format for the CIA repository.

SCPUSER DD

Specifies the output file for the SCPUSER type data record in CA Datacom load format for the CIA repository.

SCPXREF DD

Specifies the output file for the SCPXREF type data record in CA Datacom load format for the CIA repository.

SHFTNEXT DD

Specifies the output file for the SHFTNEXT type data record in CA Datacom load format for the CIA repository.

SMSINFO DD

Specifies the output file for the SMSINFO type data record in CA Datacom load format for the CIA repository.

SMSXREF DD

Specifies the output file for the SMSXREF type data record in CA Datacom load format for the CIA repository.

SRCREC DD

Specifies the output file for the SRCREC type data record in CA Datacom load format for the CIA repository.

SYSINFO DD

Specifies the output file for the SYSINFO type data record in CA Datacom load format for the CIA repository.

TIMEINFO DD

Specifies the output file for the TIMEINFO type data record in CA Datacom load format for the CIA repository.

TIMEREC DD

Specifies the output file for the TIMEREC type data record in CA Datacom load format for the CIA repository.

UDFCHAR DD

Specifies the output file for the UDFCHAR type data record in CA Datacom load format for the CIA repository.

UDFDATE DD

Specifies the output file for the UDFDATE type data record in CA Datacom load format for the CIA repository.

UDFNUM DD

Specifies the output file for the UDFNUM type data record in CA Datacom load format for the CIA repository.

UDFTIME DD

Specifies the output file for the UDFTIME type data record in CA Datacom load format for the CIA repository.

UIDXREF DD

Specifies the output file for the UIDXREF type data record in CA Datacom load format for the CIA repository.

USERACF2 DD

Specifies the output file for the USERACF2 type data record in CA Datacom load format for the CIA repository.

USERCICS DD

Specifies the output file for the USERCICS type data record in CA Datacom load format for the CIA repository.

USERDCE DD

Specifies the output file for the USERDCE type data record in CA Datacom load format for the CIA repository.

USERGRP DD

Specifies the output file for the USERGRP type data record in CA Datacom load format for the CIA repository.

USERIDMP DD

Specifies the output file for the USERIDMP type data record in CA Datacom load format for the CIA repository.

USERINFO DD

Specifies the output file for the USERINFO type data record in CA Datacom load format for the CIA repository.

USERKBLK DD

Specifies the output file for the USERKBLK type data record in CA Datacom load format for the CIA repository.

USERKERB DD

Specifies the output file for the USERKERB type data record in CA Datacom load format for the CIA repository.

USERLANG DD

Specifies the output file for the USERLANG type data record in CA Datacom load format for the CIA repository.

USERLNTE DD

Specifies the output file for the USERLNTE type data record in CA Datacom load format for the CIA repository.

USERLNX DD

Specifies the output file for the USERLNX type data record in CA Datacom load format for the CIA repository.

USERNDS DD

Specifies the output file for the USERNDS type data record in CA Datacom load format for the CIA repository.

USERNETV DD

Specifies the output file for the USERNETV type data record in CA Datacom load format for the CIA repository.

USERNODE DD

Specifies the output file for the USERNODE type data record in CA Datacom load format for the CIA repository.

USERNVCL DD

Specifies the output file for the USERNVCL type data record in CA Datacom load format for the CIA repository.

USERNVDM DD

Specifies the output file for the USERNVDM type data record in CA Datacom load format for the CIA repository.

USEROMVS DD

Specifies the output file for the USEROMVS type data record in CA Datacom load format for the CIA repository.

USEROPED DD

Specifies the output file for the USEROPER type data record in CA Datacom load format for the CIA repository.

USEROPMS DD

Specifies the output file for the USEROPMS type data record in CA Datacom load format for the CIA repository.

USERSECL DD

Specifies the output file for the USERSECL type data record in CA Datacom load format for the CIA repository.

USERTSO DD

Specifies the output file for the USERTSO type data record in CA Datacom load format for the CIA repository.

USERTSS DD

Specifies the output file for the USERTSS type data record in CA Datacom load format for the CIA repository.

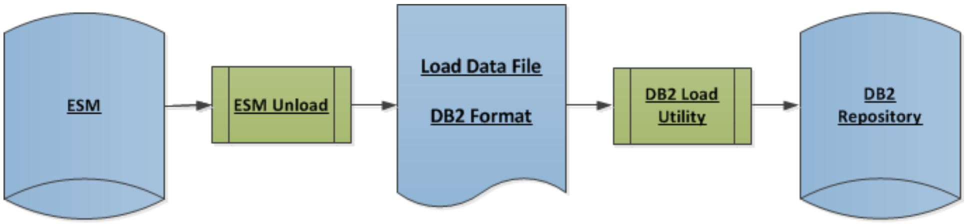
USERVM DD

Specifies the output file for the USERVM type data record in CA Datacom load format for 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.

Follow these steps:

1. Edit the CIALOAD job in CIA.CAK0JCL0, changing it to conform to your installation standards and directing it to the target DB2 subsystem where the repository is defined.

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

   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.

   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.

Chapter 5: Compliance Information Analysis Reports

A set of compliance information analysis reports is provided as part of the CIA feature of the CA Top Secret product. These reports process the data in the security repository to provide report information typically needed during a compliance assessment of a security implementation.

Benefits of the Compliance Reports

The information in the security repository is a replication of the information from the security database, which is generally accessible using CA Top Secret commands. However, the information in the security repository has been designed and resolved specifically to service compliance reporting. Using compliance reports generated from the security repository provides the following benefits:

- The compliance reports present all of the compliance information required for compliance assessment in an organized and easy to understand format. To otherwise obtain the same information, many different CA Top Secret commands must be issued, and the information correlated manually.
- Because the information in the security repository has been designed and resolved specifically to service the compliance reports, the compliance reports generally run much more quickly than the CA Top Secret commands required to provide the same compliance information.
- In a multiple system environment, the compliance reports can be run for more than one system image at a time. To obtain the same information, CA Top Secret commands must be issued in each system image and the information correlated manually.

Software Requirements

The compliance reports distributed as part of the CIA feature are written in CA Easytrieve, a fourth-generation programming language product. A subset of the CA Easytrieve product is provided as a component of CA Common Services (CCS). This Common Services component must be installed and configured before the compliance reports can be run.

When the compliance reports request information from the CIA security repository, CA Easytrieve uses CA Pan/SQL to retrieve the information from CA Datacom or DB2. CA Pan/SQL is a separate component and is provided as part of the package for [set to your product name]. This component must be installed and configured before the compliance reports can be run.

For more information, see Installing the CA Common Services Easytrieve Component and Installing the CA-PAN/SQL Interface.

Concepts for the Compliance Reports

The documentation for the compliance reports contains some terminology that may not be familiar to a user of the security product. This section describes the concepts that underlie the terminology. Verify that you understand these concepts before running the compliance reports.

SYSID

The security repository can contain the security information from multiple security images, that is, multiple security databases. The information from each system image is uniquely identified with a system ID, or SYSID. Each table in the repository has a column for the SYSID value. This column is used to identify, for each row in the table, the system to which the information belongs.

By default, the Unload utility uses the four character system identification from the z/OS SMCA control block as the SYSID value. To provide a different, possibly more meaningful, for the SYSID columns in the repository, specify the SYSID parameter in the Unload utility

Global IDs

The security repository can contain the security information from multiple security images, that is, multiple security databases. An individual user can have userids on one or more of those images, and can have multiple userids on a single system. The concept of a global ID is used to associate every userid for an individual user with that user, regardless of the userid and the security image it is defined on. For example, an individual user can have two userids TESTID1 and TESTID2 on a system image SYSTEMT, and one userid PRODID1 on a system image SYSTEMP. All of these userids can be identified to the individual user with the definition of a global ID.

A global ID for the user is defined in the IDMAP table of the security repository. The table entries associate each of the userids in each of the system images with that global ID. In the previous example, a global ID GLBLID1 is defined in the IDMAP table with entries associating userid TESTID1 on SYSTEMT, TESTID2 on SYSTEMT, and PRODID1 on SYSTEMP with the global ID.

With this mechanism a user can be identified with the global ID, and reports and inquiries can be performed for each security image with all of the userids associated with the user.

Roles

The role is the basic precept of the best-practice security architecture named role-based security. Role-based security is a way of grouping users for access authorization, which provides for easier administration and a simpler, more-easily understood security policy.

In a role-based security implementation, access authorization to a resource is not given to the individual users who require access. Instead, roles are identified that have a common set of responsibilities and requirements. For each role, the set of users that share the role is identified. For example, all people in a specific job position may share the same set of responsibilities and have the same authorization requirements. The job position is identified as a role and the people in that job position are identified as sharing the role.

In a role-based security implementation, a security role is defined for a common set of authorization requirements. Access authorization is given once to the role, rather than individually to each user. The users who perform in the role are attached to the role in the security model. By being attached to the role, a user acquires all of the access authorizations given to the role. Users typically have a set of roles that they perform in their job function, and are attached to the corresponding set of roles in the security model.

When a new user is provisioned, instead of being given access authorizations for each resource that they require, they are attached to the roles that correspond to their job requirements. If a user changes job function, they are detached from the role or roles that correspond to their old job function and attached to the role or roles that correspond to their new job function. When a user is de-provisioned, they are detached from all role or roles, which removes all of their access authorizations. They may also be removed from the security database.

In the security model for CA Top Secret, profiles are the implementation of role-based security. Profiles are defined with the CREATE command, and resource access authorizations are permitted to the profiles. Users are attached to a profile with the ADDTO command and detached with the REMOVE command. In this documentation, when a role is referenced, it will be understood as referencing a profile.

JCL and Common Control Parameters

The following sections describe JCL and common control parameters.

Sample JCL

Sample JCL for running each of the reports is provided in the CAI.CAK0JCL0 data set. The following table shows the CAK0JCL0 member names, along with the program names and the report titles.

Member Name	Program Name	Report Title
CIARPT01	CAS4CR01	List Roles By User
CIARPT02	CAS4CR02	List Users By Role
CIARPT03	CAS4CR03	List Roles and Users By Resource
CIARPT04	CAS4CR04	List Resources By Role or User
CIARPT05	CAS4CR05	List Administrative Authority By Resource
CIARPT06	CAS4CR06	List Resources by Data Classification

Report Output

Report output is written to the file in the RPTOUT DD statement in the compliance report JCL. This report output is 133 characters per line.

Control Parameter Syntax

Input control parameters are read from the file in the CNTLCARD DD statement in the compliance report JCL. These control parameter statements must have a record length of 80.

The following is the structure of the control parameter statements for the compliance reports:

- The control parameter keyword must begin in column 1.
- The parameter value for the control parameter keyword must begin in column 10.

To add comments to the input control statements, place an asterisk (‘*’) in column 1.

Common Control Parameters

The following are the common control parameters and their descriptions.

SYSID Control Statement—Specify Systems for Report

Each of the distributed compliance reports has a SYSID control statement.

SYSID

Determines the system scope of the report by specifying the system or systems whose information is processed for the report. The SYSID control statement can contain a specific SYSID value, or it can contain a masked value requesting information from more than one system.

The masking supported for this value is the following SQL request masking:

- The underscore character ('_') is a mask for a single character
- The percent character ('%') is a mask for zero or more characters.

SYSID is the only control statement that can be masked.

Example

This example requests that the compliance report include information for any system whose SYSID value begins with the characters 'SI':

```
SYSID(SI%)
```

CLASS Control Statement—Specify Class of Resources for Report

Several of the distributed compliance reports have a CLASS control statement.

Class

Determines the scope of the report by specifying the class of resources for which the report is requested.

Limits: Must be the one-to-eight character value specified for the type of resource in the ADDTO or PERMIT commands.

Example

This example shows the the resource class for data sets:

```
DATASET
```

RESOURCE Control Statement—Specify Resources for Report

Several of the distributed compliance reports have a RESOURCE control statement.

RESOURCE

Determines the scope of the report by specifying the resource or set of resources for which the report is requested.

Limits: The RESOURCE value in this control statement is not maskable, but can be a partial resource name (see the PREFIX parameter).

PREFIX Control Statment—Specify Resource Parameter Value Type

The distributed compliance reports that have a RESOURCE control statement also have a PREFIX control statement.

PREFIX Y|N

Specifies the type of value that was provided in the RESOURCE parameter. If the PREFIX parameter value is set to Y (yes), the RESOURCE parameter value is treated as a prefix and matches any resource entity in the repository that begins with the RESOURCE value or a corresponding mask. If the PREFIX parameter value is set to N (no), the RESOURCE parameter value is treated as a full resource name and only matches resource entities in the repository for the full resource name or a corresponding mask.

ROLE Control Statement—Specify Role Profile for Report

Several of the distributed compliance reports have a ROLE control statement.

Role

Determines the scope of the report by specifying the specific role profile for which the report is requested.

USERNAME Control Statement—Display User Name in Report

Several of the distributed compliance reports have a USERNAME control statement.

USERNAME Y|N

Specifies whether to display the user name associated with each userid in the report.

LINECNT Control Statement—Set Number of Lines per Page

Each of the distributed compliance reports has a LINECNT control statement.

LINECNT

Defines the number of lines per page in the report.

Compliance Report - List Roles By User

The compliance report lists the roles for a specific user or for all users.

The report can be customized in the following ways:

- The report can be requested for a single system image or for multiple system images.
- The report can be requested for a single user or for all users.
- If the report is requested for a specific user, it can identify the user in one of two ways:
  - With a specific userid
  - With a global ID, which is used to determine the userids that correspond to the user
- If the report is requested for all userids, the userids can be grouped by userid or by global ID.
- The user name can be displayed for the userids listed in the report.
- If there are calendar constraints on the user connection to the profile, they can be displayed.

This report can be used to answer the following compliance questions:

- For a user, what profiles are connected to the user?
- What user ACIDs are defined and what profiles are connected to each user?
- If there are calendar constraints on the user and profile connection, what are they?

Benefits of the Compliance Report

For a single userid, the information in the compliance report can be obtained by issuing the following command:

```
TSS LIST(acid)
```

For all userids, the information in this report can be obtained by issuing the following command:

```
TSS LIST(acids)
```

The advantages of the report over issuing the CA Top Secret commands include:

- In a multiple system image environment, the report can be run for more than one system image. To obtain the same information using the TSS command, the command must be issued in each system image, and the information then correlated manually.
- If a user has more than one ACID in a single system image, or different ACIDs in different system images, the report can be run using a global ID. The global ID obtains each ACID associated with the user, and reports on the profiles connected to each ACID.
- The report displays only the profiles connected to the user. The TSS command displays additional information, and the connected profiles must be extracted from the information.
- The compliance report for all userids and the connected profiles can be requested at any time, and runs quickly with no impact on security product performance. The TSS command to obtain the same information must process the entire security database. This command takes a long time, impacts performance of the security product, and should only be run during periods of low activity.

Input Parameter Syntax

the input parameter syntax follows:

```
SYSID     SYSID mask
USERID    userid
ALLUSERS  Y|N
GLOBALID  globalid
ALLGBLS   Y|N
LINECNT   number
DATES     Y|N
```

Input Parameters

SYSID

Specifies the SYSID or SYSID mask of the system or systems whose information is processed for the report. The SYSID parameter can contain a specific SYSID value, or it can contain a masked value requesting information from more than one system.

The masking supported for this value follows DB2 SQL request masking:

- The underscore character ('_') is a mask for a single character.
- The percent character ('%') is a mask for zero or more characters.

Limits: one to eight characters

Example: SYSID(SI%) requests that the compliance report include information for any system whose SYSID value begins with the characters 'SI'.

USERID, ALLUSERS, GLOBALID, ALLGBLS

One of the following parameters is required. They are mutually exclusive, so only one can be specified.

USERID

Specifies a userid for which the roles will be listed.

ALLUSERS Y|N

Lists all userids with the roles that are connected to each userid.

Default: N

GLOBALID

Specifies a global ID for the report request. All of the userids associated with the global ID are listed, with the roles that are connected to each userid.

ALLGBLS Y|N

Lists all global IDs. For each global ID, each userid associated with the global ID is listed, with the roles that are connected to the userid.

Default: N

USERNAME Y|N

(Optional) Specifies that the NAME associated with each userid should be displayed in the report.

Default: N

DATES Y|N

(Optional) Specifies that any active and expire dates for a role, as well as any userid's expire date for a role, should be displayed in the report.

Default: N

LINECNT number_

(Optional) Specifies the number of lines per page in the report.

Default: 60

Limits: numbers from 10 to 9999999999999999

DATES Y|N

(Optional) Specifies that any active and expire dates for a role, as well as any userid's expire date for a role, and the user expire date associated with each ACID, should be displayed in the report. If the date displayed is determined to be past the system CURRENT DATE, an *EXPIRED* message is displayed next to the date value on the report.

Default: N

List Roles By User: Sample Report Input

The following input parameters are specified for the sample report:

```
//CNTLCARD DD *
* List all roles for userid THORI32
* for all SYSIDs that start with SY
SYSID    SY%
USERID   THORI32
USERNAME Y
LINECNT  60
```

These control parameters ask the report to do the following:

1. Process the information for any system image that starts with ‘SY’.
2. Display all roles for userid THORI32.
3. List the user name and the userid.

List Roles By User: Explanation of Report Output

The first page of the report includes the date and time that the report was run, the report title, and the input parameters that were used. The remaining sections of the report include the SYSID and the security product name, the userid, the user name, the LPAR (specified as ESMsysid), and all the roles for the userid. A count of the roles for the userid is given at the end of each section.

Sample Report Output

```
2/22/2007 11.21.04        Compliance Information Report - List Roles By User      Page     1

Input Parameters
----------------
SYSID    = SY%
USERID   = THORI32
USERNAME = Y


2/22/2007 11.21.04        Compliance Information Report - List Roles By User      Page     2
                              Compliance Information for USERID: THORI23

SYSID: SYSA     PRODUCT: CA Top Secret
NAME: RICHARD THOMPSON

Roles for this user:
--------------------
PROD0001                  OPER0001                  TEST0001

      3  roles are defined for this user

================================================================================================

SYSID: SYSB     PRODUCT: CA Top Secret
NAME: RICHARD THOMPSON

Roles for this user:
--------------------
PROD0001                  OPER0001                  TEST0001                  DEV01

      4  roles are defined for this user
```

Compliance Report - List Users By Role

The List Users By Role report lists all of the users connected to a specific role, or all of the roles that are defined and the users connected to each role.

The report can be customized with the following controls:

- The report can be requested for a single system image or for multiple system images.
- The report can be requested for a single role or for all roles.
- The report can display the user name for the userids listed in the report.

This report can be used to answer the following compliance questions:

1. For a specific profile, what users are connected to the profile?
2. What profiles are defined, and what users are connected to each profile?
3. If calendar constraints exist for the user and profile connection, what are they?

Benefits of the List Users by Role Report

For a specific profile, the list users by role report is equivalent to issuing the following command:

```
TSS LIST(profile) DATA(ACIDS)
```

For all profiles, this report is equivalent to issuing the following command:

```
TSS LIST(ACIDS) DATA(ACIDS) TYPE(PROFILE)
```

Advantages of the report over the CA Top Secret commands include:

- In a multiple system image environment, the report can be run for more than one system image. To obtain the same information using the TSS command, the command must be issued in each system image and the information correlated manually.
- The report for all profiles and the connected users can be requested at any time and runs quickly with no performance impact. The TSS command to obtain the same information has to process the entire security database. This command takes a long time to execute, impacts the performance of the security product, and should only be run during periods of low activity.
- The report provides the ability to list the name fields for the connected userids. To obtain the same information using the TSS command, each userid must be listed individually and the information correlated manually.

Input Parameter Syntax

```
SYSID    SYSID mask
ROLE     rolename
ALLROLES Y|N
USERNAME Y|N
LINECNT  number
DATE     Y|N
```

Input Parameters

SYSID

Specifies a SYSID or SYSID mask of the system or systems whose information is processed for the report. The SYSID parameter can contain a specific SYSID value, or it can contain a masked value requesting information from more than one system.

The masking supported for this value is the following DB2 SQL request masking:

- The underscore character (‘_’) is a mask for a single character.
- The percent character (‘%’) is a mask for zero or more characters.

Limits: One to eight characters

Example: SYSID(SI%) requests that the compliance report include information for any system whose SYSID value begins with the characters ‘SI’.

ROLE, ALLROLES

One of these parameters is required. They are mutually exclusive, so only one can be specified.

ROLE

Specifies a profile name. All ACIDs connected to this profile will be listed in the report.

ALLROLES Y|N

Specifies that all profiles that are defined should be listed, with the ACIDs that are connected to each profile.

Default: N

USERNAME Y|N

(Optional) Specifies whether the NAME associated with each userid should be displayed in the report.

Default: N

LINECNT *number*

(Optional) Specifies the number of lines per page in the report.

Default: 60

Limits: Numbers from 10 to 9999999999999999

DATES Y|N

(Optional) Specifies whether any active and expire dates for a role, as well as any userid's expire date for a role, and the user expire date associated with each ACID, should be displayed in the report. If the date displayed is past the system CURRENT DATE, an *EXPIRED* message is displayed next to the date value on the report.

Default: N

Sample Report Input

The following input parameters are specified for the sample report:

```
//CNTLCARD DD *
* List userids and names for a given role
* for all SYSIDs that start with SY.
SYSID    SY%
ROLE     PROFILE9
USERNAME Y
LINECNT  60
```

These control parameters ask the report to do the following:

- Process information for any system image whose SYSID starts with ‘SY.’
- Display all users connected to the PROFILE9 profile.
- Display the user name with the userids.

List Users By Role: Explanation of Report Output

The first page of the report includes the date and time that the report was run, the report title and the input parameters that were used. The remaining sections of the report include the SYSID and the security product name on the second title line. The role name is displayed, followed by the userids that have the role and the corresponding user name. A count of the userids within the role is given at the end of each section.

Sample Report Output

```
2/22/2007 10.54.30          Compliance Information Report - List Users By Role      Page       1

Input Parameters
----------------
SYSID    = SY%
ROLE     = PROFILE9
USERNAME = Y

2/22/2007 10.54.30          Compliance Information Report - List Users By Role      Page      2
                  Compliance Information for System:  SYSA      Product:  CA Top Secret

ROLE : PROFILE9

Userid   Name                        Userid   Name                  Userid   Name
-------- -------------------------   -------- --------------------- -------- --------------------
ACFSEC01 MARY PERKINS                ACFSEC02 BOB DOLITTLE          COMDO12  DOT COMM
DONBI32  BILL DONALDSON              LANHA05  HARVEY LANG           SMIEL09  ELLEN SMITH

       6  users are in this role

===============================================================================================
2/22/2007 10.54.30         Compliance Information Report - List Users By Role        Page     3
                 Compliance Information for System:  SYSB      Product:  CA Top Secret

ROLE : PROFILE9
Userid   Name                        Userid   Name                  Userid   Name
-------- -------------------------   -------- --------------------- -------- --------------------
ACFSEC01 MARY PERKINS                ACFSEC02 BOB DOLITTLE          COMDO12  DOT COMM
DONBI32  BILL DONALDSON

       4  users are in this role

===============================================================================================
```

Compliance Report - List Roles and Users by Resource

The List Roles and Users by Resource report lists the roles and users who have access to a specific resource and the conditions under which access is permitted.

The report can be customized with the following controls:

- The report can be requested for a single system image or for multiple system images.
- The report can be request for a single resource or for a set of resources with a common prefix value.
- The report can include roles and users who have access to the resource, not through policy, but through special user attributes that override policy recommendations.
- For roles that have access to the resource, the report can include the list of users connected to the role.
- For users who have access to the resource, the report can include the user name field.
- For resource authorizations that have time, day, and date controls, the report can include time, day, and date information.

This report can be used to answer the following compliance questions:

- What users and profiles have access to the resource through special attributes?
- What users and profiles have access to the resource through ownership, either of the best fit resource entity or of a different masked resource entity?
- What users and profiles have access to the resource through PERMITs, either through the best fit resource entity or through a different masked resource entity?
- For profiles that have access to the resource, who are the users that have access because they are connected to a profile?

Benefits of the List Roles and Users by Resource

The base CA Top Secret product has no equivalent to the List Roles and Users by Resource report. The closest equivalent is the TSS WHOHAS command, which shows the users and profiles that have access to the resource through PERMITs on the best-fit owned resource entity. This command does not list users and profiles that have access to the resource through special attributes or through resource ownership. The command also does not list users and profiles that have access rights through owned and permitted resources other than the best-fit resource entity. For profiles that have access through PERMITs, it does not list the users who have access because they are connected to the profile. Some of this information can be obtained through other TSS commands, but obtaining it is a long manual process.

The advantages of the report over issuing CA Top Secret commands are as follows:

- In a multiple system image environment, the report can be run for more than one system image. To obtain the same information using TSS commands, the commands must be issued for each system image, and the information correlated manually.
- In a single process, you can obtain all users who have access to the resource for any reason, a process that would be tedious, difficult, and possibly incomplete using TSS commands.
- The report can be customized to return the depth of information desired.

Input Parameter Syntax

```
SYSID    SYSID mask
CLASS    resource class
RESOURCE resource entity
PREFIX   Y|N
USERIDS  Y|N
USERNAME Y|N
SPECIAL  Y|N
DATETIME Y|N
LINECNT  number
```

Input Parameters

SYSID

Specifies the SYSID or SYSID mask of the system or systems whose information is processed for the report. The SYSID parameter can contain a specific SYSID value or a masked value requesting information from more than one system.

The masking supported for this value is the following DB2 SQL request masking:

- The underscore character ('_') is a mask for a single character
- The percent character ('%') is a mask for zero or more characters.

For example, SYSID(SI%) requests that the compliance report include information for any system whose SYSID value begins with the characters 'SI.'

Limits: 1 to 8 characters

CLASS

Specifies the resource class of the requested resource.

The value for the CLASS parameter must be the value specified for the type of resource in the ADDTO or PERMIT commands. For example, the resource class for data sets is DATASET.

Limits: 1 to 8 characters. This parameter is not maskable.

RESOURCE

Specifies the resource or set of resources for which the report is requested.

When RESOURCE is long, it may be broken up onto multiple lines with this format:

```
RESOURCE SOME.RESOURCE.NAMES.MUST.
         SPAN.MULTIPLE.LINES.BECAUSE.THEY.CAN.
         CONTAIN.UP.TO.256.CHARACTERS
```

Note: The RESOURCE parameter should not be split by any other parameter lines. Blanks in columns 1 – 9 assume a continued RESOURCE parameter.

Limits: This parameter is not maskable, but may be a partial resource name (if PREFIX Y is also specified).

PREFIX Y|N

(Optional) Specifies the kind of value was provided in the RESOURCE control statement. If the PREFIX parameter value is set to Y (yes), the RESOURCE parameter value is treated as a prefix, and will match any resource entity in the repository that begins with the RESOURCE value or a corresponding mask. If the PREFIX parameter value is set to N (no), the RESOURCE parameter value is treated as a full resource name, and will only match resource entities in the repository for the full resource name or a corresponding mask.

Default: N

USERIDS Y|N

(Optional) Specifies whether, when a role has access to the resource, a list of all userids connected to the role appears in the report.

Default: N

USERNAME Y|N

(Optional) Specifies if the NAME associated with each useried appears in the report. If USERNAME Y is specified with USERIDS N, the USERNAME parameter is ignored.

Default: N

SPECIAL Y|N

(Optional) Specifies whether a section of the report is generated listing userids that have access to the resource, not through resource policy, but through special user attributes.

Default: N

DATETIME Y|N

(Optional) Specifies whether the date and time restrictions that modify the access authorization, if any, are displayed. If DATETIME N is specified, the date and time control name is displayed, but the corresponding date and time restrictions are not displayed.

Default: N

LINECNT number

(Optional) Specifies the number of lines per page in the report.

Default: 60

Limits: 10 to 999999999999999999

List Roles and Users By Resource: Sample Report Input

The following input parameters are specified for the report:

```
//CNTLCARD DD *
* List accesses for all datasets that
* start with SYS1 in the CIA repository.
SYSID    %
CLASS    DATASET
RESOURCE SYS1
PREFIX   Y
USERIDS  Y
USERNAME Y
SPECIAL  Y
DATETIME Y
```

These control parameters ask the report to do the following:

1. Process information for any system image
2. Display access authorizations for all data sets that start with the characters 'SYS1'
3. Display a list of users that are connected to the role, for any role that has access to the resource
4. Display the user name for any userid listed in the report
5. Display a report section for users who have access because of special user attributes
6. Display the specific date and time restrictions associated with an access authorization

Explanation of List Roles and Users by Resource Report

The first page of the report shows the date and time that the report was run, the report title and the input parameters that were used.

The second section of the report shows the userids and user names for the users who have access because of special user attributes.

The third section of the report shows the profiles that have access because of special attributes on the profile itself, and the userids and user names of users connected to the profiles.

The fourth section of the report shows access due to resource policy (resource ownership and PERMITs). The resource ownership is shown first, followed by the information for any matching PERMITs. When a profile has access to the resource, the userids and user names are displayed for the users that are connected to the profile. A separator line of equal signs ('=') separates the information for each owned resource, and a separator line of dashes ('-') separates the information for each matching PERMIT for the owned resource.

Sample Report Output

```
2/26/2007 16.23.28     Compliance Information Report - Roles and Users by Resource     Page    1

Input Parameters
----------------
SYSID    = %
CLASS    = DATASET
RESMASK  = SYS1
PREFIX   = Y
USERIDS  = Y
USERNAME = Y
SPECIAL  = Y

2/26/2007 16.23.28    Compliance Information Report - Roles and Users by Resource     Page     2
                 Compliance Information for System:  SYSB      Product:  CA Top Secret
                                    Userids with Access Due to Special Privileges

Userid   Username                         Privileges
-------- -------------------------------- ---------------------------------------
BOBDO02  BOB DOLITTLE                     NODSNCHK
COMDO12  DOT COMM                         NODSNCHK
DONBI32  BILL DONALDSON                   NODSNCHK
GRABI37  BILL GRASSER                     NODSNCHK
LANHA05  HARVEY LANG                      NODSNCHK
MARYP01  MARY PERKINS                     NODSNCHK
MONJO24  JOE MONTANA                      NODSNCHK
MSCAGUY  MASTER                           NODSNCHK          MSCA
SCHRO35  RODNEY SCHNITZ                   NODSNCHK
MSCAGUY  MASTER SECURITY                  NODSNCHK
VANAR32  ART VANDELAY                     NODSNCHK

===============================================================================================

PROFILE:      ABCD0001         PRIVILEGES:  NODSNCHK  MODE(WARN)
USERID(S) with access through this profile:


USERID   USERNAME                  USERID   USERNAME              USERID   USERNAME
-------- -------------------------  -------- ---------------------  -------- ------------------
BOBDO02  BOB DOLITTLE              COMDO12  DOT COMM              DONBI32  BILL DONALDSON
GRABI37  BILL GRASSER              LANHA05  HARVEY LANG           MARYP01  MARY PERKINS
MONJO24  JOE MONTANA               MONJO24  JOE MONTANA           SCHRO35  RODNEY SCHNITZ
SMIEL09  ELLEN SMITH               STEAN92  ANNIE STEVENS

            11   users match this PROFILE.

===============================================================================================
PROFILE:      ABCD1234         PRIVILEGES:  NODSNCHK  MODE(DORM)
USERID(S) with access through this profile:
```

```
              No users match this PROFILE.

2/26/2007 16.23.28    Compliance Information Report - Roles and Users by Resource     Page   3
                 Compliance Information for System:  SYSB      Product:  CA Top Secret

                                 Access Due to Policy
===============================================================================================
CLASS:       DATASET       OWNED RESOURCE:  ++
OWNER:       MSCAGUY
-----------------------------------------------------------------------------------------------
RESMASK:     ++
USERID:      USER13                  NAME:  TEST USER11
ACCESS:      READ(ALLOW)
ACTIONS:     No actions found.
===============================================================================================
CLASS:       DATASET       OWNED RESOURCE:  *.
OWNER:       MSCAGUY
-----------------------------------------------------------------------------------------------
RESMASK:     *.
USERID:      MSCAGUY                 NAME:  MASTER SECURITY
ACCESS:      ALL(ALLOW)
ACTIONS:     No actions found.
-----------------------------------------------------------------------------------------------
RESMASK:     *.PARMLIB.
PROFILE:     BCDE0022
ACCESS:      UPDATE(ALLOW)
ACTIONS:     No actions found.
USERID(S) with access:
              No users match this PROFILE.
-----------------------------------------------------------------------------------------------
RESMASK:     SYS1.
PROFILE:     BCDE0033
ACCESS:      READ(ALLOW)
ACTIONS:     EXIT

USERID(S) with access:

USERID   USERNAME                    USERID   USERNAME               USERID   USERNAME
-------- -------------------------   -------- ---------------------  -------- ------------------
BOBDO02  BOB DOLITTLE                COMDO12  DOT COMM               DONBI32  BILL DONALDSON
GRABI37  BILL GRASSER                LANHA05  HARVEY LANG            MARYP01  MARY PERKINS
MONJO24  JOE MONTANA                 MONJO24  JOE MONTANA            SCHRO35  RODNEY SCHNITZ

             9   users match this PROFILE.
-----------------------------------------------------------------------------------------------
RESMASK:     SYS1.PROCLIB
PROFILE:     SYSTEMP
ACCESS:      UPDATE(ALLOW) CREATE(ALLOW) DBMAINT(ALLOW)
ACTIONS:     EXIT
```

```
USERID(S) with access:

USERID   USERNAME                   USERID   USERNAME              USERID   USERNAME
-------- -------------------------  -------- --------------------  -------- ------------------
MONJO24  JOE MONTANA                MONJO24  JOE MONTANA           SCHRO35  RODNEY SCHNITZ
SMIEL09  ELLEN SMITH                VANAR32  ART VANDELAY
             5   users match this PROFILE.
===============================================================================================
```

Compliance Report - List Resources by Role or User

The List Resources by Role or User report lists all of the resources that a specific role or userid has access to, and the conditions under which access is permitted.

The report can be customized with the following controls:

- The report can be requested for a single system image or for multiple system images.
- The report can be requested for a specific user or a specific role.
- If the report is for a specific user, that user can be identified in one of two ways:
  - With a userid
  - With a global ID, which is used to determine the userids that correspond to the user
- The report can identify special attributes for the role or user that permit the role or user access to resources regardless of specific policy recommendations.
- For users who are listed for a system image or global ID, the report can include the user name field.
- For resource authorizations that have time, day, and date controls, the report can include time, day, and date information.
- The report can include or omit information about resources that are permitted to all users.

This report answers the following compliance questions:

- For a user or profile, what special attributes does the user or profile have that permit access regardless of specific policy recommendations?
- For a user or profile, what resources does the user or profile have access to through resource ownership?
- For a user or profile, what resources does the user or profile have access to through resource policy (PERMITs) and under what conditions?

Benefits of the List Resources by Role or User

The List Resources by Role or User report is generally equivalent to the TSS LIST(acid) command, which shows the attributes, resource ownership, and resource access permitted to the user or profile.

Advantages of the report over issuing CA Top Secret commands are:

- In a multiple system image environment, the report can be run for more than one system image. To obtain the same information using the TSS command, the command must be issued in each system image and the information correlated manually.
- If a user has more than one ACID in a single system image, or different ACIDs in different system images, the report can be run using a global ID. This obtains each ACID associated with the user, and reports on the resources authorized for each ACID. To obtain the same information using the TSS command report, the command must be issued for each ACID and the information correlated manually.
- The report displays only the resource access information for the role or user. The TSS command displays additional information, and the special attributes, resource ownership, and resource authorizations must be extracted from the information.

Input Parameter Syntax

```
SYSID    SYSID mask
ROLE     rolename
USERID   userid
GLOBALID globalid
USERNAME Y|N
SPECIAL  Y|N
ALL      Y|N
DATETIME Y|N
LINECNT  number
DATE     Y|N
```

Input Parameters

SYSID

Specifies a SYSID or SYSID mask of the system or systems whose information is processed for the report. The SYSID parameter can contain a specific SYSID value, or it can contain a masked value requesting information from more than one system.

The masking supported for this value is the DB2 SQL request masking:

- The underscore character ('_') is a mask for a single character
- The percent character ('%') is a mask for zero or more characters.

Limits: One to eight characters

Example: SYSID(SI%) requests that the compliance report include information for any system whose SYSID value begins with the characters 'SI'.

USERID, GLOBALID, ROLE

One of these parameters is required. They are mutually exclusive, so only one can be specified.

USERID

Specifies the userid for the report request.

GLOBALID

Specifies the global ID for the report request. All of the userids associated with the global ID will be processed for the report.

ROLE

Specifies a profile for the report request.

USERNAME Y|N

(Optional) Specifies whether the NAME associated with the specified userid is displayed in the report. If a ROLE is specified, this parameter is ignored.

Default: N

ALL Y|N

(Optional) Specifies whether the report includes information about resources that are permitted to all users. If a ROLE is specified and you want to see only the resource accesses permitted to the specified profile, specify ALL=N.

Default: Y

SPECIAL Y|N

(Optional) Specifies whether the section of the report is generated listing special attributes for the role or user that permit the role or user access to resources regardless of specific policy recommendations. These special attributes include the MSCA, NORESCHK, and NODSNCHK attributes and the MODE field.

Default: N

DATETIME Y|N

(Optional) Specifies whether the date and time restrictions that modify the access authorization, if any, are displayed. If DATETIME N is specified, the date and time control name is displayed, but the corresponding date and time restrictions are not displayed.

Default: N

LINECNT number

(Optional) Specifies the number of lines per page in the report.

Limits: numbers from 10 to 999999999999999999

Default: 60

DATES Y|N

(Optional) Specifies if any active and expire dates for a role, any userid's expire date for a role, and the user expire date associated with each ACID, appear in the report. If the date displayed in the report is past the system CURRENT DATE, an *EXPIRED* message is displayed next to the date value on the report.

Default: N

Sample Report Input

The following input parameters are specified for the list resources by role or user report:

```
//CNTLCARD DD *
* List all of the resources that role TESTPRF1
* has access to on systems that start with SY.
SYSID      SY%
ROLE      TESTPRF1
USERNAME  Y
SPECIAL   Y
LINECNT   60
```

These control parameters ask the report to do the following:

- Process information for any system image whose SYSID starts with ‘SY.'
- Display all resources to which profile TESTPRF1 has access authorization.
- Display a report section listing special attributes of the userid|profile that give access authorization to resources regardless of resource policy.
- Display the user name for the userid specified on the report. However, this parameter is ignored because a role is specified.

Explanation of Report Output

The first page of the report shows the date and time that the report was run, the report title and the input parameters that were used.

The second section shows access due to ownership. In this case profile TESTPRF1 owns TESTUSER. in CLASS DATASET.

The third section shows access due to policy. This section shows any permits that grant the user access. Access and action types are shown. The access is displayed in the format ACCESS: access_type(ALLOW). The access_type is the type of access that was specified on the PERMIT. If the access_type is NONE, access is not allowed to this resource.

Sample Report Output

```
3/06/2007 10.52.38    Compliance Information Report - Resource by Role or User     Page    1

Input Parameters
----------------
SYSID    = SY%
ROLE     = TESTPRF1
USERNAME = Y
SPECIAL  = Y
LINECNT  = 60


3/06/2007 10.52.38    Compliance Information Report - Resource by Role or User    Page    2
                               Compliance Information for ROLE:  TESTPRF1
                 Compliance Information for System:  SYSB      Product:  CA Top Secret

                                    Access Due to Ownership

================================================================================================
CLASS:       DATASET       OWNED RESOURCE:  TESTUSER.
OWNER:       TESTPRF1
================================================================================================

3/06/2007 10.52.38     Compliance Information Report - Resource by Role or User    Page    3
                              Compliance Information for ROLE:  TESTPRF1
                    Compliance Information for System:  SYSB     Product:  CA Top Secret

                                   Access Due to Policy
================================================================================================
CLASS:       ABCTABLE      OWNED RESOURCE:  X14D48
OWNER:       VIPGUY01
------------------------------------------------------------------------------------------------
RESMASK:     X14D48.PAY1
PROFILE:     TESTPRF1
ACCESS:      READ(ALLOW)
ACTIONS:     No actions found.
------------------------------------------------------------------------------------------------
RESMASK:     X14D48.PAY2
PROFILE:     *ALL*
ACCESS:      No access found.
ACTIONS:     EXIT
=================================================================================================
CLASS:       DATASET       OWNED RESOURCE:  SYS.
OWNER:       VIPGUY
-------------------------------------------------------------------------------------------------
RESMASK:     SYS1.
PROFILE:     TESTPRF1
ACCESS:      UPDATE(ALLOW)
ACTIONS:     No actions found.
```

```
------------------------------------------------------------------------------------------------
RESMASK:     SYSINFO.
PROFILE:     *ALL*
ACCESS:      READ(ALLOW)
ACTIONS:     No actions found.
=================================================================================================
```

Compliance Report - Administrative Authority by Resource

The Administrative Authority by Resource report lists all of the users that have the authority to define or modify the security policy for a specific resource or set of resources.

The report can be customized with the following controls:

- The report can be requested for a single system image or for multiple system images.
- The report can be requested for a single resource or for a set of resources with a common prefix value.
- The report can include users who can perform administration for the resource, not through administrative scope, but through special user attributes.
- For users who can perform administration for the resource, the report can include the user name field.

This report answers the following compliance questions:

- What users can perform administration for the resource through special attributes?
- What users can perform administration for the resource through administrative scope?
- What users can perform administration for the resource through resource ownership, either of the best-fit resource entity or of a different masked resource entity?
- If a profile can perform administration for the resource through resource ownership, who are the users that have administrative access because they are connected to the profile?

Benefits of the Compliance Report

There is no complete equivalent to the Administrative Authority by Resource report in base CA Top Secret product. The closest equivalent is the TSS WHOOWNS command, which displays the user or profile that can perform administration through ownership on the best-fit owned resource entity. However, this command does not list users that have administrative authority for the resource through special attributes or through administrative scope. It does not list users or profiles that have administrative access through owned resources other than the best-fit resource entity. For profiles that have administrative authority, it does not list the users who have administrative authority because they are connected to the profile. Some of this information can be obtained from other TSS commands, but running these commands would be a long manual process.

Advantages of the report include:

- In a multiple system image environment, the report can be run for more than one system image. To obtain the same information using TSS commands, each command must be issued for every system image, and the information correlated manually.
- In a single process, you can obtain all users who can perform administration for the resource for any reason, a process that would be tedious, difficult, and possibly incomplete using TSS commands.
- The report can be customized to return the depth of information desired.

Administrative Authority By Resource Report: Input Parameter Syntax

```
SYSID    sysidmask
CLASS    resourceclass
RESOURCE resource
PREFIX   Y|N
USERNAME Y|N
SPECIAL  Y|N
LINECNT  number
```

Input Parameters

SYSID

Specifies the SYSID or SYSID mask of the system or systems whose information is processed for the report. The SYSID parameter can contain a specific SYSID value or it can contain a masked value requesting information from more than one system.

The masking supported for this value is the following DB2 SQL request masking:

- The underscore character (‘_’) is a mask for a single character.
- The percent character (‘%’) is a mask for zero or more characters.

For example, SYSID(SI%) requests that the compliance report include information for any system whose SYSID value begins with the characters ‘SI’.

Limits: 1 to 8 characters.

CLASS

Specifies the resource class of the requested resource. The value for the CLASS parameter must be the value specified for the type of resource in the ADDTO or PERMIT commands. For example, the resource class for data sets is DATASET.

Limits: 1 to 8 characters. This parameter is not maskable.

RESOURCE

Specifies the resource or set of resources for which the report is requested.

Limits: The RESOURCE value is not maskable, but may be a partial resource name (if PREFIX Y is also specified). RESOURCE may be broken out onto multiple lines with this format:

```
RESOURCE SOME.RESOURCE.NAMES.MUST.
         SPAN.MULTIPLE.LINES.BECAUSE.THEY.CAN.
         CONTAIN.UP.TO.256.CHARACTERS
```

The RESOURCE parameter should not be split by any other parameter lines. Blanks in columns 1 – 9 indicate a continued RESOURCE parameter.

PREFIX Y|N

(Optional) Specifies what kind of value was provided in the RESOURCE control statement. If the PREFIX parameter value is set to Y (yes), the RESOURCE parameter value is treated as a prefix, and will match any resource entity in the repository that begins with the RESOURCE value or a corresponding mask. If the PREFIX parameter value is set to N (no), the RESOURCE parameter value is treated as a full resource name, and only matches resource entities in the repository for the full resource name or a corresponding mask.

Default: N

USERIDS Y|N

(Optional) Specifies whether, when a profile has administrative authority for the resource, a list of all userids connected to the profile appear in the report.

Default: N

USERNAME Y|N

(Optional) Specifies whether the NAME associated with each userid is displayed in the report. If USERNAME Y is specified with USERIDS N, the USERNAME parameter is ignored.

Default: N

SPECIAL Y|N

(Optional) Specifies whether a section of the report is generated listing userids that have administrative authority for the resource through special user attributes.

SPECIAL Y causes a section of the report to be generated displaying userids with the following special privileges:

- MSCA Type ACIDS
- SCA Type ACIDS that can administer resources in the input resource class

Default: N

LINECNT number

(Optional) Specifies the number of lines per page in the report.

Defaults: 60

Limits: 10 to 999999999999999999

Administrative Authority By Resource Report: Sample Report Input

The following input parameters are specified for the report:

```
//CNTLCARD DD *
* List administrative authorities for all datasets that
* start with CI for all SYSIDs that start with SY
SYSID    SY%
CLASS    DATASET
RESOURCE CI
PREFIX   Y
USERNAME Y
SPECIAL  Y
LINECNT  60
```

These control parameters ask the report to do the following:

1. Process information for any system image whose SYSID starts with ‘SY’
2. Display all users with administrative authority for any data set starting with ‘CI’

3. Display a report section listing users who have administrative authority because of special attributes
4. Display the user name for any userid listed in the report

Explanation of Report Output

The first page of the report shows the date and time that the report was run, the report title and the input parameters that were used.

The second section shows all userids with administrative authority due to special privileges. This page is only shown when the SPECIAL input parameter is Y (YES). The MSCA userid and name is displayed first. Next are listed the SCAs that can administer the input CLASS and also have OWN or XAUTH or both.

Note: An SCA appears twice when that SCA has administrative authority over the specific CLASS and ALL resource classes. However, these SCAs are only counted once in the final count.

The third section of the report shows the class, the matching owned resource and its owner. These are followed by any USERs, DCAs, VCAs, ZCAs, or LSCAs that have OWN or XAUTH privileges for the resource class. The SCOPEID column shows the organizational ACID such as department name, division name, or zone name.

Sample Report Output

```
2/26/2007 10.27.13 Compliance Information Report - Roles and Users by Resource  Page  1

Input Parameters
----------------
SYSID    = SY%
CLASS    = DATASET
RESOURCE = CI
PREFIX   = Y
USERNAME = y
SPECIAL  = Y
LINECNT  = 60


2/22/2007 10.27.13 Compliance Information Report - Administrative Authority By Resource Page 2
                 Compliance Information for System:  SYST      Product:  CA Top Secret
                          Userids with Administrative Authority Due to Special Privileges

MSCA Userid: BIGGUY27                  Name: MASTER SECURITY
===============================================================================================
SCA Userids:

USERID    NAME                              OWN  XAUTH  CLASS
--------  --------------------------------  ---  -----  --------
GRABI37   BILL GRASSER                       Y     Y    *ALL*
MONJO24   JOE MONTANA                        Y     Y    DATASET
SCHRO35   RODNEY SCHNITZ                     Y     Y    DATASET
SCHRO35   RODNEY SCHNITZ                     Y     Y    *ALL*
STEAN92   ANNIE STEVENS                      Y     Y    DATASET
STEAN92   ANNIE STEVENS                      Y     Y    *ALL*

           4  unique SCA Userids were found.

2/22/2007 10.27.13 Compliance Information Report - Administrative Authority By Resource Page 3
                Compliance Information for System:  SYST      Product:  CA Top Secret
                                    Userids with Administrative Authority

CLASS: DATASET   OWNED RESOURCE: ++
OWNER: BIGGUY27

There are no DCA, VCA, ZCA or LSCA Userids with administrative authority for this owned resource.

------------------------------------------------------------------------------------------------
CLASS: DATASET   OWNED RESOURCE: *.
OWNER: BIGGUY27

There are no DCA, VCA, ZCA or LSCA Userids with administrative authority for this owned resource.

------------------------------------------------------------------------------------------------
```

```
CLASS: DATASET   OWNED RESOURCE: CIA.
OWNER: SCOMA05

USERID    NAME                              SCOPEID   TYPE  OWN  XAUTH  CLASS
--------  --------------------------------  --------  ----  ---  -----  --------
MARYP01   MARY PERKINS                      DEPT1829  DCA    Y     Y    DATASET
BOBDO02   BOB DOLITTLE                      DIV1829   VCA    Y     Y    *ALL*
COMDO12   DOT COMM                          ZONE1829  ZCA    Y     Y    DATASET
DONBI32   BILL DONALDSON                    ZONE1829  LSCA   Y     Y    *ALL*
LANHA05   HARVEY LANG                       ZONE1829  LSCA   Y     Y    *ALL*
SMIEL09   ELLEN SMITH                       ZONE1829  LSCA   Y     Y    *ALL*

         6  Userids have administrative authority for this owned resource.
-----------------------------------------------------------------------------------------------
```

Compliance Report - Data Classification and Ownership

The Data Classification and Ownership report lists the data class and ownership information of system resources as defined by the Data Class Ownership (DCO) records. The report can be customized with the following controls:

- The report can be requested for a single system image or for multiple system images.
- The report can be requested for a single data class or for all data classes.

This report displays for each data class, and all the record IDs, descriptions, resource classes, resource masks, and ownership information that match the input parameters. This report can be useful when evaluating of the data classification and ownership information for resources in a CA Top Secret environment.

Benefits of the List Roles By User

This report is equivalent to issuing the TSS List (dataclas) command. The advantage of the compliance report over issuing the TSS command is:

- In a multiple system image environment, the report can be run for more than one system image. To obtain the same information using TSS commands, each command must be issued for every system image, and the information correlated manually.
- In a single process, you can obtain a list of all users who can perform administration for the resource for any reason, a process that would be tedious, difficult, and possibly incomplete using TSS commands.
- The report can be customized to return the depth of information desired.

Data Classification and Ownership: Input Parameter Syntax

```
SYSID   sysidmask
DCLASS  dclassmask
LINECNT number
```

Data Classification and Ownership: Input Parameters

SYSID *sysidmask*

Specifies a one- to eight-character SYSID or SYSID mask of the system or systems whose information is processed for the report. The SYSID parameter can contain a specific SYSID value, or it can contain a masked value requesting information from more than one system.

The masking supported for this value is the following SQL request masking:

- The underscore character ('_') is a mask for a single character.
- The percent character ('%') is a mask for zero or more characters.

Example: SYSID(SI%)

This example requests that the compliance report include information for any system whose SYSID value begins with the characters 'SI'.

The SYSID parameter is required.

DCLASS *dclassmask*

Specifies a 1- to 32-character Data Class or Data Class mask of the systems whose information is processed for the report. The DCLASS parameter can contain a specific Data Class value or it can contain a masked value requesting information from more than one Data Class.

This value supports the following SQL request masking:

- The underscore character ('_') is a mask for a single character.
- The percent character ('%') is a mask for zero or more characters.

Example: DCLASS(SOX%)

This example requests that the compliance report include information for any Data Class whose DCLASS value begins with the characters 'SOX'.

The DCLASS parameter is required.

LINECNT *number*

(Optional) Specifies the number of lines per page in the report.

Default: 60

Limits: 10 - 99999999999999999

Data Classification and Ownership: Sample Report Input

The following input parameters are specified for the report:

```
//CNTLCARD DD *
SYSID   XE%
DCLASS  %
```

These control parameters ask the report to do the following:

1. Process information for any system image whose SYSID starts with 'XE'
2. Display all data classes defined for each system image.

Explanation of Report Output

The first page of the Data Classification and Ownership report includes the date and time that the report was run, the report title, the input parameters that were used and a table of the system images processed for this report.

The second section includes each data class with a detailed list of all the Dataclass records, including the resource and ownership information defined for the data class. The total number of DCO records processed is concluded for each data class.

The third section of the report totals the number of data classes and the number of DCO records processed for each system image.

Sample Report Output

```
12/11/2008 11.12.29              Compliance Information Report - Resource by Data Classification
Page       1

 Input Parameters
 ----------------
 SYSID    = XE%
 DCLASS   = %

 Systems in the repository matching the requested SYSID:

 Sysid     Application Name          Application Version       Load Date
 --------  ------------------------  ------------------------  ----------
 XE43      CA Top Secret             Release 14.0              2008-12-10

12/11/2008 11.12.29              Compliance Information Report - Resource by Data Classification
Page       2
                                   Data Class Records for System:  XE43     Product:  CA Top Secret


=================================================================================================
==============================

 Data Class:   HIPPA

=================================================================================================
==============================

 Recid:        DATA.HIPPA4
 Description:  HEALTH INFO PRIVACY ACT
 Resclass:     DATASET
 Resmask:      CEO0001.-
 Owner1:       CEO0001
 Owner1 Name:  DR. CEO

 Recid:        DATA.SECURITY
 Description:  HOMELAND SECURITY AGENCY
 Resclass:     DATASET
 Resmask:      CIA*.-
 Owner1:       CIO0001
 Owner1 Name:  CHIEF INFORMATION OFFICER
 Owner2:       OPER001
 Owner2 Name:  SYSTEMS OPERATOR

 Recid:        DATA.HIPPA3
 Description:  HEALTH INFO PRIVACY ACT
 Resclass:     DATASET
 Resmask:      CIAMSTR.-
 Owner1:       CEO0001
 Owner1 Name:  DR. CEO

 Recid:        DATA.HIPPA1
 Description:  HEALTH INFO PRIVACY ACT
 Resclass:     DATASET
 Resmask:      CIASCAX1.-
 Owner1:       CEO0001
 Owner1 Name:  DR. CEO

 Recid:        DATA.HIPPA2
 Description:  HEALTH INFO PRIVACY ACT
 Resclass:     DATASET
 Resmask:      CIAX2.-
 Owner1:       CEO0001
 Owner1 Name:  DR. CEO

     Number of DCO records for the data class:                      5

==================================================================================================
==============================

 Data Class:   SECURITY_CLASS

==================================================================================================
==============================

12/11/2008 11.12.29              Compliance Information Report - Resource by Data Classification
Page       3
                                   Data Class Records for System:  XE43     Product:  CA Top Secret

 Recid:        DATA.SECURITY
 Description:  HOMELAND SECURITY AGENCY
 Resclass:     DATASET
 Resmask:      CIA*.-
 Owner1:       CIO0001
 Owner1 Name:  CHIEF INFORMATION OFFICER
 Owner2:       OPER001
 Owner2 Name:  SYSTEMS OPERATOR

      Number of DCO records for the data class:                      1

==================================================================================================
==============================

 Data Class:   SOX

==================================================================================================
==============================
 Recid:         DATA.SECURITY
 Description:   HOMELAND SECURITY AGENCY
 Resclass:      DATASET
 Resmask:       CIA*.-
 Owner1:        CIO0001
 Owner1 Name:   CHIEF INFORMATION OFFICER
 Owner2:        OPER001
 Owner2 Name:   SYSTEMS OPERATOR

 Recid:         DATA.SOX1
 Description:   SARBANES-OXLEY ACT
 Resclass:      DATASET
 Resmask:       CIA1.-
 Owner1:        JANE
 Owner1 Name:   MRS. JANE SAND
 Owner2:        MASTER
 Owner2 Name:   MR. JOHN DOE

 Recid:         DATA.SOX2
 Description:   SARBANES-OXLEY ACT
 Resclass:      DATASET
 Resmask:       CIA2.-
 Owner1:        JANE
 Owner1 Name:   MRS. JANE SAND
 Owner2:        MASTER
 Owner2 Name:   MR. JOHN DOE

 Recid:         DATA.SOX3
 Description:   SARBANES-OXLEY ACT
 Resclass:      DATASET
 Resmask:       CIA3.-
 Owner1:        JANE
 Owner1 Name:   MRS. JANE SAND
 Owner2:        MASTER
 Owner2 Name:   MR. UNIVERSE

112/11/2008 11.12.29             Compliance Information Report - Resource by Data Classification
Page       4
                                  Data Class Records for System:  XE43     Product:  CA Top Secret

 Recid:         DATA.SOX4
 Description:   SARBANES-OXLEY ACT
 Resclass:      DATASET
 Resmask:       CIA4.-
 Owner1:        JANE
 Owner1 Name:   MRS. JANE SAND
 Owner2:        MASTER
 Owner2 Name:   MR. JOHN DOE
```

```
     Number of DCO records for the data class:                     5

-------------------------------------------------------------------------------------------------
-----------------------------
     Total number of data classes for sysid:                       3

     Total number of DCO records for sysid:                        9
```

Chapter 6: Examples of Ad-Hoc SQL Queries

One advantage of externalizing the security information into a relational repository is that the information becomes available for ad-hoc queries using SQL. Queries that run a long time or that have a performance impact when run against the active security database can be easily run against the information in the security repository.

Because the repository is not used in security processing, intensive queries can be run with no impact on the performance of the security product. Because most of the data in the relational repository has been resolved and indexed, queries that run a long time in the base security environment are processed much quicker. In addition, custom queries cannot be serviced in the base security environment without writing programs that use the security product programming interface. These queries can be created and run against the information in the security repository.

This chapter contains examples of some SQL queries, shows how to write a query, and how the query would be serviced from the repository information.

This section contains the following topics:

List Roles Connected to a Userid

This SQL query is the foundation of the CAS4CR01 report. This query returns all of the roles that are connected to a specific userid on a specific system image.

The ROLEXREF table contains the cross-reference information matching a role with each userid connected to the role.

To list roles connected to a userid, execute the following SQL commands:

```
SELECT *
FROM   CIADB01.ROLEXREF
WHERE USERID = 'TESTU01' AND
      SYSID= 'SY59';
```

A report with the roles connected to a userid is created.

List Users Connected to a Role

This SQL query is the foundation of the CAS4CR02 report. This query returns the userids and user names for all users who are connected to a specific role on a specific image.

The ROLEXREF table contains the cross-reference information matching a role with each userid connected to the role. The USERINFO table is used to return the user name for the userid.

To list users connected to a role, run the following SQL commands:

```
SELECT CIADB01.ROLEXREF.SYSID, CIADB01.ROLEXREF.USERID, NAME
FROM   CIADB01.ROLEXREF, CIADB01.USERINFO
WHERE ROLEID  = 'PROFILE1' AND
      CIADB01.ROLEXREF.SYSID = 'SY59' AND
      CIADB01.ROLEXREF.SYSID = CIADB01.USERINFO.SYSID AND
      CIADB01.ROLEXREF.USERID = CIADB01.USERINFO.USERID
      ORDER BY SYSID, USERID;
```

A report with users connected to the specified role is created.

List Userids for a Global ID

This SQL query returns all the userids associated with a specific global ID for all the system images represented in the repository.

The IDMAP table contains the cross-reference information matching a global ID with each userid and system image combination that corresponds to that global ID. The USERINFO table is used to return the user name for the userid.

```
SELECT CIADB01.IDMAP.SYSID , CIADB01.IDMAP.USERID, NAME
FROM   CIADB01.IDMAP, CIADB01.USERINFO
WHERE GLOBALID = 'TESTU01' AND
      CIADB01.IDMAP.SYSID LIKE '%' AND
      CIADB01.IDMAP.SYSID = CIADB01.USERINFO.SYSID AND
      CIADB01.IDMAP.USERID = CIADB01.USERINFO.USERID
      ORDER BY SYSID, USERID;
```

List Users Who Have Been Inactive

This query lists the userid and user name field for every userid that has been inactive in the last thirty days, for all of the system images represented in the repository.

The USERINFO table contains fields for the system ID, the userid, the user name, and the last accessed date for the userid.

```
SELECT SYSID, USERID, NAME, LUDATE
FROM   CIADB01.USERINFO
WHERE DAYS(CURRENT DATE) - DAYS(LUDATE) + 1 > 30
ORDER BY SYSID, USERID;
```

List Users Who Have Been Defined in the Last Thirty Days

This query lists the userid and the user name field for every userid that was defined in the last thirty days, for all of the system images represented in the repository.

The USERINFO table contains fields for the system ID, the userid, the user name, and create date for the userid.

```
SELECT SYSID, USERID, NAME, CREDATE
FROM   CIADB01.USERINFO
WHERE DAYS(CURRENT DATE) - DAYS(CREDATE) + 1 < 30
ORDER BY SYSID, USERID;
```

Chapter 7: CIA Service Functions

This section contains the following topics:

About Table Functions

The CIA feature contains ten CIA user-defined table functions. Table functions can be used in the FROM clause of an SQL SELECT statement. Each function returns a table of rows from a specific table. The returned table matches input criteria based on the masking rules of the CA Top Secret product.

CAISEC.CIA_FILTER_MATCH Table Function

The CAISEC.CIA_FILTER_MATCH table function returns rows from the PERMXREF table that match the input parameters of the function. It calls the CAISEC.CIA_RESOURCE_MATCH function and filters the table rows that it returns. CA Top Secret related rows are returned without further filtering.

```
CAISEC.CIA_FILTER_MATCH(in-resource, in-resource-type, in-resource-sysid,
in-prefix)
```

```
RETURNS TABLE( sysid, resclass, rulekey, authid, seqnum, resmask, noprefix, prefix,
nextkey, authtype, append, adminby, admindate, admintime, active,  until, acc-read,
acc-write, acc-allocate, acc-add, acc-update,  acc-delete, acc-execute, acc-all,
acc-alter, acc-alterin, acc-bind,  acc-copy, acc-create, acc-createin, acc-cretab,
acc-crets, acc-dbadm,  acc-dbcntl, acc-dbmaint, acc-dispdb, acc-drop, acc-dropin,
acc-imagecopy,  acc-index, acc-insert, acc-load, acc-packadm, acc-recovdb,
acc-refer,  acc-reorg, acc-repair, acc-select, acc-startdb, acc-stats, acc-stopdb,
acc-trigger, acc-usage, actn-audt, actn-exit, actn-fail, actn-ntfy,  actn-vrfy,
actn-nods, mode, ddname, volume, dayrecid, timerecid,  srcrecid, data, db2sysid )
```

The schema is CAISEC.

in-resource

Specifies the name of a resource used for matching resource masks in the PERMXREF table. The name can be either a full name or a partial name (prefix). The data type is VARCHAR.

Limits: maximum length of 256 bytes

in-resource-type

Specifies the resource class or type of the input resource. The data type is VARCHAR.

Limits: Maximum length 8 bytes

in-resource-sysid

Specifies a sysid used to limit results to the systems in question. This parameter accepts SQL wildcard characters (% and _) for pattern matching. The data type is VARCHAR.

Limits: Maximum length 8 bytes

in-prefix

Indicates whether the in-resource parameter is a full or partial resource name. Valid values are PREFIX or NOPREFIX. PREFIX indicates that the in-resource parameter is the beginning of a resource name, and will match any resource masks in the PERMXREF table that begin with this prefix. NOPREFIX indicates that the in-resource parameter is a full resource name and only resource masks that match the entire name are returned. The data type is VARCHAR.

Limits: Maximum length 8 bytes

CAISEC.CIA_RESOURCE_MATCH: Returned Columns

This function returns a CIA table with the following columns. Some column values can be null.

SYSID	VARCHAR(8)
RESCLASS	CHAR(8)
RULEKEY	VARCHAR(256)
AUTHID	CHAR(24)
SEQNUM	SMALLINT
RESMASK	VARCHAR(256)
NOPREFIX	CHAR(1)
PREFIX	VARCHAR(40)
NEXTKEY	VARCHAR(40)
AUTHTYPE	CHAR(1)
APPIND	CHAR(1)
ADMINBY	CHAR(8)
ADMINDATE	DATE
ADMINTIME	TIME
ACTIVE	DATE
UNTIL	DATE
ACC_READ	CHAR(1)
ACC_WRITE	CHAR(1)
ACC_ALLOCATE	CHAR(1)
ACC_ADD	CHAR(1)
ACC_UPDATE	CHAR(1)
ACC_DELETE	CHAR(1)
ACC_EXECUTE	CHAR(1)
ACC_ALL	CHAR(1)
ACC_ALTER	CHAR(1)
ACC_ALTERIN	CHAR(1)
ACC_BIND	CHAR(1)
ACC_COPY	CHAR(1)
ACC_CREATE	CHAR(1)
ACC_CREATEIN	CHAR(1)
ACC_CRETAB	CHAR(1)
ACC_CRETS	CHAR(1)
ACC_DBADM	CHAR(1)
ACC_DBCNTL	CHAR(1)
ACC_DBMAINT	CHAR(1)
ACC_DISPDB	CHAR(1)
ACC_DROP	CHAR(1)
ACC_DROPIN	CHAR(1)
ACC_IMAGECOPY	CHAR(1)
ACC_INDEX	CHAR(1)
ACC_INSERT	CHAR(1)
ACC_LOAD	CHAR(1)
ACC_PACKADM	CHAR(1)
ACC_RECOVDB	CHAR(1)

```
ACC_REFER     CHAR(1)
ACC_REORG     CHAR(1)
ACC_REPAIR    CHAR(1)
ACC_SELECT    CHAR(1)
ACC_STARTDB   CHAR(1)
ACC_STATS     CHAR(1)
ACC_STOPDB    CHAR(1)
ACC_TRIGGER   CHAR(1)
ACC_USAGE     CHAR(1)
ACTN_AUDT     CHAR(1)
ACTN_EXIT     CHAR(1)
ACTN_FAIL     CHAR(1)
ACTN_NTFY     CHAR(1)
ACTN_VRFY     CHAR(1)
ACTN_NODS     CHAR(1)
MODE          CHAR(1)
DDNAME        CHAR(8)
VOLUME        CHAR(6)
DAYRECID      CHAR(12)
TIMERECID     CHAR(12)
SRCRECID      CHAR(8)
DATA          VARCHAR(64)
DB2SYSID      CHAR(4)
```

CAISEC.CIA_FILTER_MATCH: Example

This example SQL statement uses the function in a FROM clause:

```
SELECT SYSID, RESCLASS, RULEKEY, RESMASK, NEXTKEY, APPIND
FROM
TABLE(CAISEC.CIA_FILTER_MATCH('TESTUSR.NEXTKEY','DATASET','%','NOPREFIX'))
AS PI1;
```

CAISEC.CIA_FILTER_MATCH: Example Result

```
---------+---------+---------+---------+---------+---------+------------+--
SYSID     RESCLASS  RULEKEY     RESMASK            NEXTKEY        APPIND
---------+---------+---------+---------+---------+---------+------------+--
XE61      DATASET   TESTUSR     TESTUSR.NEXTKEY.-  TESTUSRN       A
XE59      DATASET   TESTUSR     TESTUSR.NEXTKEY.-  TESTUSRN       A
XE59      DATASET   TESTUSR     TESTUSR.-                         A
XE59      DATASET   TESTUSR     TESTUSR.-                         A
XE61      DATASET   TESTUSR     TESTUSR.-                         A
XE61      DATASET   TESTUSR     TESTUSR.-                         A
XE61      DATASET   TESTUSR     TESTUSR.-                         A
XE59      DATASET   TESTUSRN    TESTUSR.-                         A
XE59      DATASET   TESTUSRN    TESTUSR.-                         A
XE31      DATASET   %.          %.                                T
XE31      DATASET   %.          %.                                T
XE31      DATASET   %.          %.                                T
XE31      DATASET   %.          %.*                               T
XE31      DATASET   %.          %.*                               T
XE31      DATASET   %.          %.*****                           T
XE31      DATASET   **          ******                            T
XE31      DATASET   **          **                                T
XE31      DATASET   *.          *.*.*.%                           T
XE31      DATASET   *.          *.*.*.%                           T
XE31      DATASET   *.          *.*.JXF                           T
XE31      DATASET   *.          *.*.*.SYSTEM12                    T
XE31      DATASET   ++          ++                                T
XE31      DATASET   *.          *.*.*.SYSTEM22                    T
```

CAISEC.CIA_RESOURCE_MATCH Table Function

This function returns rows from the PERMXREF table that match the input parameters of the function.

The schema is CAISEC.

Syntax

This function has the following format:

```
CAISEC.CIA_RESOURCE_MATCH(in-resource, in-resource-type, in-resource-sysid,
in-prefix)
```

Return Values

This function returns the following values:

```
RETURNS TABLE(sysid, resclass, rulekey, authid, seqnum, resmask, noprefix, prefix, nextkey, authtype,
append, adminby, admindate, admintime, active, until, acc-read, acc-write, acc-allocate, acc-add,
acc-update, acc-delete, acc-execute, acc-all, acc-alter, acc-alterin, acc-bind, acc-copy, acc-create,
acc-createin, acc-cretab, acc-crets, acc-dbadm, acc-dbcntl, acc-dbmaint, acc-dispdb, acc-drop,
acc-dropin, acc-imagecopy, acc-index, acc-insert, acc-load, acc-packadm, acc-recovdb, acc-refer,
acc-reorg, acc-repair, acc-select, acc-startdb, acc-stats, acc-stopdb, acc-trigger, acc-usage,
actn-audt, actn-exit, actn-fail, actn-ntfy, actn-vrfy, actn-nods, mode, ddname, volume, dayrecid,
timerecid, srcrecid, data, db2sysid)
```

Parameters

This function has the following parameters:

in-resource

Defines the name of a resource used for matching resource masks in the PERMXREF table. The name can be either a full name or a partial name (prefix). The data type is VARCHAR:

Limits: Maximum length 256 bytes

in-resource-type

Defines the resource class or type of the input resource. The data type is VARCHAR.

Limits: Maximum length 8 bytes

in-resource-sysid

Defines a sysid used to limit results to the systems in question. This parameter accepts SQL wildcard characters (% and _) for pattern matching. The data type is VARCHAR.

Limits: Maximum length 8 bytes

in-prefix

Specifies whether the in-resource parameter is a full or partial resource name. Valid values are PREFIX or NOPREFIX. PREFIX specifies that the in-resource parameter is the beginning of a resource name, and matches any resource masks in the PERMXREF table that begin with this prefix. NOPREFIX specifies that the in-resource parameter is a full resource name and only resource masks that match the entire name are returned. The data type is VARCHAR.

Limits: Maximum length 8 bytes

CAISEC.CIA_RESOURCE_MATCH: Returned Columns

This function returns a CIA table with the following columns. Some column values can be null.

SYSID	VARCHAR(8)
RESCLASS	CHAR(8)
RULEKEY	VARCHAR(256)
AUTHID	CHAR(24)
SEQNUM	SMALLINT
RESMASK	VARCHAR(256)
NOPREFIX	CHAR(1)
PREFIX	VARCHAR(40)
NEXTKEY	VARCHAR(40)
AUTHTYPE	CHAR(1)
APPIND	CHAR(1)
ADMINBY	CHAR(8)
ADMINDATE	DATE
ADMINTIME	TIME
ACTIVE	DATE
UNTIL	DATE
ACC_READ	CHAR(1)
ACC_WRITE	CHAR(1)
ACC_ALLOCATE	CHAR(1)
ACC_ADD	CHAR(1)
ACC_UPDATE	CHAR(1)
ACC_DELETE	CHAR(1)
ACC_EXECUTE	CHAR(1)
ACC_ALL	CHAR(1)
ACC_ALTER	CHAR(1)
ACC_ALTERIN	CHAR(1)
ACC_BIND	CHAR(1)
ACC_COPY	CHAR(1)
ACC_CREATE	CHAR(1)
ACC_CREATEIN	CHAR(1)
ACC_CRETAB	CHAR(1)
ACC_CRETS	CHAR(1)
ACC_DBADM	CHAR(1)
ACC_DBCNTL	CHAR(1)
ACC_DBMAINT	CHAR(1)
ACC_DISPDB	CHAR(1)
ACC_DROP	CHAR(1)
ACC_DROPIN	CHAR(1)
ACC_IMAGECOPY	CHAR(1)
ACC_INDEX	CHAR(1)
ACC_INSERT	CHAR(1)
ACC_LOAD	CHAR(1)
ACC_PACKADM	CHAR(1)
ACC_RECOVDB	CHAR(1)

```
ACC_REFER     CHAR(1)
ACC_REORG     CHAR(1)
ACC_REPAIR    CHAR(1)
ACC_SELECT    CHAR(1)
ACC_STARTDB   CHAR(1)
ACC_STATS     CHAR(1)
ACC_STOPDB    CHAR(1)
ACC_TRIGGER   CHAR(1)
ACC_USAGE     CHAR(1)
ACTN_AUDT     CHAR(1)
ACTN_EXIT     CHAR(1)
ACTN_FAIL     CHAR(1)
ACTN_NTFY     CHAR(1)
ACTN_VRFY     CHAR(1)
ACTN_NODS     CHAR(1)
MODE          CHAR(1)
DDNAME        CHAR(8)
VOLUME        CHAR(6)
DAYRECID      CHAR(12)
TIMERECID     CHAR(12)
SRCRECID      CHAR(8)
DATA          VARCHAR(64)
DB2SYSID      CHAR(4)
```

CAISEC.CIA_RESOURCE_MATCH: Example

This example SQL statement uses the function in a FROM clause:

```
SELECT SYSID, RESCLASS, RULEKEY, RESMASK, NETXKEY, APPIND
 FROM
 TABLE(CAISEC.CIA_RESOURCE_MATCH('SYS1.PARMIB','DATASET','%','NOPREFIX'))
 AS PI1;
```

CAISEC.CIA_RESOURCE_MATCH: Example Result

```
---------+---------+---------+---------+---------+---------+------------+--

SYSID     RESCLASS  RULEKEY     RESMASK          NEXTKEY        APPIND

---------+---------+---------+---------+---------+---------+------------+--

XE61      DATASET   DSNPOST     *-.-                               A
XE61      DATASET   NOBROWN1    *-.-             NOBROWN2          A
XE61      DATASET   NOBROWN2    *-.-             NOBROWN3          A
XE61      DATASET   NOBROWN3    *-.-             NOBROWN4          A
XE61      DATASET   NOBROWN4    *-.-             NOBROWN5          A
XE61      DATASET   NOBROWN5    *-.-                               A
XE61      DATASET   PRODSYS     SYS1.PARMLIB                       A
XE61      DATASET   PRODSYS     SYS1.-                             A
XE61      DATASET   RSPA        -.-.-                              A
XE31      DATASET   ++          ++                                 T
XE31      DATASET   *.          *.*.*.%                            T
XE31      DATASET   *.          *.*.*.%                            T
XE31      DATASET   *.          *.*.*.SYSTEM12                     T
XE31      DATASET   *.          *.*.*.SYSTEM22                     T
XE31      DATASET   *.          *.*.SYSTEM12                       T
XE31      DATASET   *.          *.*.SYSTEM22                       T
XE31      DATASET   **          **                                 T
XE31      DATASET   %.          %.*                                T
XE31      DATASET   %.          %.*****                            T
XE31      DATASET               SYSSYS1.PARMLIB                    T
XE31      DATASET               SYSSYS1.PARMLIB                    T
```

CAISEC.CIA_ROLEINFO_MATCH Table Function

This function returns rows from the ROLEINFO table that matches the input parameters of the function.

The schema is CAISEC.

Syntax

This function has the following format:

```
CAISEC.CIA_ROLEINFO_MATCH(in-uid, in- uid -sysid)
```

Return Values

This function returns the following values:

```
RETURNS TABLE(sysid ,roleid, expdate, actdate)
```

Parameters

This function has the following parameters:

in-uid

Defines the uid used for matching uid masks in the ROLEINFO table. The data type is VARCHAR.

Limits: Maximum length 24 bytes

in-uid-sysid

Defines a sysid used to limit results to the systems in question. This parameter accepts SQL wildcard characters (% and _) for pattern matching. The data type is VARCHAR.

Limits: Maximum length 8 bytes

CIASEC.CIA_SCOPERES_MATCH: Returned Columns

This function returns a CIA table with the following columns. Some column values can be null.

```
SYSID VARCHAR(8)
ROLEID VARCHAR(24)
EXPDATE DATE
ACTDATE DATE
```

CAISEC.CIA_ROLEINFO_MATCH: Example

This example SQL statement uses the function in a FROM clause:

```
SELECT *
FROM
TABLE(CAISEC.CIA_ROLEINFO_MATCH('     T    ','%'))
AS PI1;
```

CAISEC.CIA_ROLEINFO_MATCH: Example Result

```
---------+---------+---------+---------+---------+---------+-
SYSID     ROLEID                    EXPDATE     ACTDATE
---------+---------+---------+---------+---------+---------+-
XE31      *****T******************  ----------  ----------
XE61      ************************  ----------  ----------
XE61      ** *********************  ----------  ----------
XE75         *********************  ----------  ----------
```

CAISEC.CIA_SCOPERES_MATCH Table Function

This function returns rows from the SCPRES table that matches the input parameters of the function.

The schema is CAISEC.

Syntax

This function has the following format:

```
CAISEC.CIA_SCOPERES_MATCH(in-resource, in-resource-type, in-resource-sysid,
in-prefix)
```

Return Values

This function returns the following values:

```
RETURNS TABLE(sysid ,scopeid, resclass, resmask, scptype, masktype, appind)
```

Parameters

This function has the following parameters:

in-resource

Defines the name of a resource used for matching resource masks in the SCPRES table. The name can be either a full name or a partial name (prefix). The data type is VARCHAR.

Limits: Maximum length 256 bytes

in-resource-type

Defines the resource class or type of the input resource. The data type is VARCHAR.

Limits: Maximum length 8 bytes

in-resource-sysid

Defines a sysid used to limit results to the systems in question. This parameter accepts SQL wildcard characters (% and _) for pattern matching. The data type is VARCHAR.

Limits: Maximum length 8 bytes

in-prefix

Specifies whether the in-resource parameter is a full or partial resource name. Valid values are PREFIX or NOPREFIX. PREFIX specifies that the in-resource parameter is the beginning of a resource name, and matches any resource masks in the PERMXREF table that begin with this prefix. NOPREFIX specifies that the in-resource parameter is a full resource name and only resource masks that match the entire name are returned. The data type is VARCHAR.

Limits: Maximum length 8 bytes

CAISEC.CIA_SCOPERES_MATCH: Returned Columns

This function returns a CIA table with the following columns. Some column values can be null.

SYSID	VARCHAR(8)
SCOPEID	VARCHAR(268)
RESCLASS	CHAR(8)
RESMASK	VARCHAR(40)
SCPTYPE	CHAR(1)
MASKTYPE	CHAR(1)
APPIND	CHAR(1)

CAISEC.CIA_SCOPERES_MATCH: Example

This example SQL statement uses the function in a FROM clause:

```
SELECT    *
 FROM
 TABLE(CAISEC.CIA_SCOPERES_MATCH('DATA.SET','DATASET','%','NOPREFIX'))
 AS PI1;
```

CAISEC.CIA_SCOPERES_MATCH: Example Result

```
---------+---------+---------+---------+---------+---------+---------+-
SYSID     SCOPEID         RESCLASS  RESMASK   SCPTYPE  MASKTYPE  APPIND
---------+---------+---------+---------+---------+---------+---------+-
XE59      DSNSCOPENEW7    DATASET   *         S        P         A
XE61      DSNSCOPESSDLRGY DATASET   *         S        P         A
XE61      LRGSCOPE        DATASET   *         S        P         A
XE61      MSH2            DATASET   ********  S        K         A
XE61      QASWBSCP        DATASET   *         S        P         A
XE61      QAUSCP          DATASET   *         S        P         A
XE61      SBSCOPE4        DATASET   *         S        P         A
XE61      SSDRCM          DATASET   *         S        P         A
XE61      TEST1           DATASET   *         S        P         A
XE61      TLCS            DATASET   *         S        P         A
XE61      TSSJHB          DATASET   *         S        P         A
XE61      UNSCOPE         DATASET   *         S        P         A
XE61      USCOPE          DATASET   *         S        P         A
```

Error Codes for CIA User-Defined Functions

This section describes the SQLSTATE values and messages returned from the CIA user-defined functions along with their respective meaning. The values are in an allowable range for CIA user applications.

For information on SQLSTATE values, see the DB2 Codes Manual.

Note: The # value for DB2 is 1 and for CA Datacom is 2.

Module CIAUFUP#/CIA4FUP# - Function CAISEC.CIA_RESOURCE_MATCH

CIAUFUP#/CIA4FUP#

Call type error

SQLSTATE Value:

38I00

Reason:

An unrecognized function call was made to the external function.

CIAUFUP#/CIA4FUP#

IN_RESOURCE length error

SQLSTATE Value:

38I01

Reason:

The input resource name has a zero length.

CIAUFUP#/CIA4FUP#

IN_RESOURCE is blank

SQLSTATE Value:

38I02

Reason:

The input resource name is blank.

CIAUFUP#/CIA4FUP#

IN_RESOURCE_TYPE length error

SQLSTATE Value:

38I03

Reason:

The input resource class or type has a zero length.

CIAUFUP#/CIA4FUP#

IN_RESOURCE_SYSID length error

SQLSTATE Value:

38I04

Reason:

The input resource sysid has a length that is either zero or greater than the maximum.

CIAUFUP#/CIA4FUP#

IN_PREFIX length error

SQLSTATE Value:

38I05

Reason:

The input prefix specification has a length that is either zero or greater than the maximum.

CIAUFUP#/CIA4FUP#

IN_PREFIX invalid

SQLSTATE Value:

38I06

Reason:

An invalid prefix specification was entered. Valid values are PREFIX or NOPREFIX.

CIAUFUP#/CIA4FUP#

DSN length error

SQLSTATE Value:

38I07

Reason:

The input data set name has a length that is either zero or greater than the maximum of 44 characters. (RESCLASS=DATASET)

CIAUFUP#/CIA4FUP#

DSN invalid

SQLSTATE Value:

38I08

Reason:

The input data set name has an invalid structure. (RESCLASS=DATASET)

CIAUFUP#/CIA4FUP#

DSN prefix length error

SQLSTATE Value:

38I09

Reason:

PREFIX with RESCLASS=DATASET but the input data set name is the maximum of 44 characters.

CIAUFUP#/CIA4FUP#

Error Converting input DSN

SQLSTATE Value:

38I10

Reason:

An error occurred formatting the input data set name for prefix processing. (RESCLASS=DATASET)

CIAUFUP#/CIA4FUP#

Error Converting Row DSN

SQLSTATE Value:

38R01

Reason:

An error occurred formatting the data set name from a table row for processing. (RESCLASS=DATASET)

CIAUFUP#/CIA4FUP#

Prefix/Rulekey length error

SQLSTATE Value:

38R02

Reason:

Both the prefix and rulekey columns from a table row have lengths of zero.

Module CIAUFUE# - Function CAISEC.CIA_SCOPERES_MATCH

CIAUFUE#

Call type error

SQLSTATE Value:

38I00

Reason:

An unrecognized function call was made to the external function.

CIAUFUE#

IN_RESOURCE length error

SQLSTATE Value:

38I01

Reason:

The input resource name has a zero length.

CIAUFUE#

IN_RESOURCE is blank

SQLSTATE Value:

38I02

Reason:

The input resource name is blank.

CIAUFUE#

IN_RESOURCE_TYPE length error

SQLSTATE Value:

38I03

Reason:

The input resource class or type has a zero length.

CIAUFUE#

IN_RESOURCE_SYSID length error

SQLSTATE Value:

38I04

Reason:

The input resource sysid has a length that is either zero or greater than the maximum.

CIAUFUE#

IN_PREFIX length error

SQLSTATE Value:

38I05

Reason:

The input prefix specification has a length that is either zero or greater than the maximum.

CIAUFUE#

IN_PREFIX invalid

SQLSTATE Value:

38I06

Reason:

An invalid prefix specification was entered. Valid values are PREFIX or NOPREFIX.

CIAUFUE#

RESMASK length error

SQLSTATE Value:

38R01

Reason:

The length of the resmask column from a table row is longer than the maximum.

Module CIAUFUC# - Function CAISEC.CIA_USERCICS_MATCH

CIAUFUC#

Call type error

SQLSTATE Value:

38I00

Reason:

An unrecognized function call was made to the external function.

CIAUFUC#

IN_USERID length error

SQLSTATE Value:

38I01

Reason:

The input userid has a zero length.

CIAUFUC#

IN_USERID is blank

SQLSTATE Value:

38I02

Reason:

The input userid name is blank.

Module CIAUFUL# - Function CAISEC.CIA_USERLANG_MATCH

CIAUFUL#

Call type error

SQLSTATE Value:

38I00

Reason:

An unrecognized function call was made to the external function.

CIAUFUL#

IN_USERID length error

SQLSTATE Value:

38I01

Reason:

The input userid has a zero length.

CIAUFUL#

IN_USERID is blank

SQLSTATE Value:

38I02

Reason:

The input userid is blank.

Module CIAUFUO# - Function CAISEC.CIA_USEROPER_MATCH

CIAUFUO

Call type error

SQLSTATE Value:

38I00

Reason:

An unrecognized function call was made to the external function.

CIAUFUO

IN_USERID length error

SQLSTATE Value:

38I01

Reason:

The input userid has a zero length.

CIAUFUO

IN_USERID is blank

SQLSTATE Value:

38I02

Reason:

The input userid is blank.

Module CIAUFUS# - Function CAISEC.CIA_USERSECL_MATCH

CIAUFUS#

Call type error

SQLSTATE Value:

38I00

Reason:

An unrecognized function call was made to the external function.

CIAUFUS#

IN_USERID length error

SQLSTATE Value:

38I01

Reason:

The input userid has a zero length.

CIAUFUS#

IN_USERID is blank

SQLSTATE Value:

38I02

Reason:

The input userid is blank.

Module CIAUFUW# - Function CAISEC.CIA_USERWRKA_MATCH

CIAUFUW#

Call type error

SQLSTATE Value:

38I00

Reason:

An unrecognized function call was made to the external function.

CIAUFUW#

IN_USERID length error

SQLSTATE Value:

38I01

Reason:

The input userid has a zero length.

CIAUFUW#

IN_USERID is blank

SQLSTATE Value:

38I02

Reason:

The input userid is blank.

Module CIAURINF - Function CAISEC.CIA_ROLEINFO_MATCH

CIAURINF

Call type error

SQLSTATE Value:

38I00

Reason:

An unrecognized function call was made to the external function.

CIAURINF

IN_UID length error

SQLSTATE Value:

38I01

Reason:

The input UID name has a zero length.

CIAURINF

IN_UID is blank

SQLSTATE Value:

38I02

Reason:

The input UID name is blank.

CIAURINF

IN_UID_SYSID length error

SQLSTATE Value:

38I04

Reason:

The input UID sysid has a length that is either zero or greater than the maximum.

CIAURINF

ROLEID length error

SQLSTATE Value:

38R01

Reason:

The length of the roleid column from a table row is longer than the maximum.

Chapter 8: GLOBALID Exit

If specified, this exit gains control in the ACID record processing module when the name of a user exit was supplied in the EXIT keyword of a GLOBALID input control statement in the unload utility SYSIN file. The user exit is a self-contained load module that must reside in the LPA.

Specification

'GLOBALID EXIT(*exitname*)' in the unload utility SYSIN file.

Attributes

AMODE(31), RMODE(ANY)

Called By

ACID record processor in the unload utility

Input

R1

Standard parameter list:

+0-Address of 8-byte userid being processed.

This section contains the following topics:

User GLOBALID Exit Paramter List (#CIAEXIT)

The #CIAEXIT macro describes the parameter list that the CA Top Secret product passes to the user globalid exit specified in the EXIT keyword of the GLOBALID input control statement in the SYSIN file.

Fields

The fields in the #CIAEXIT parameter list are as follows:

IAXTACID

The 8-byte userid currently being processed.

IAXT_GID

A 32-byte globalid returned to the caller.

IAXT_PLN

Two-byte actual length of the #CIAEXIT parameter list.

Output

The globalid returned by the user exit in the IAXT_GID field of the #CIAEXIT parameter list.

Chapter 9: Configuring CIA Real-Time Processing for CA Chorus

This section contains the following topics:

CA Chorus

CA Chorus is a management solution that delivers a role-based interaction model. CA Chorus integrates features across multiple products and disciplines, provides rich visualization, and facilitates collaboration and knowledge sharing among mainframe staff. CA Chorus helps reduce the complexity of managing mission-critical mainframe workloads and increases the productivity of your mainframe staff.

CA Chorus Security Role

CA Chorus for Security and Compliance Management lets you simplify security management for your ESM users. By focusing on a role-based delivery model, CA Chorus for Security and Compliance Management transforms the way IT staff collaborates with colleagues, interacts with management tools, and leverages the mainframe.

The CA Chorus for Security and Compliance Management role offers these usability features:

- Time series data graphing
- Real-time reporting
- Real-time access to state and event data
- Security data model extension
- Policy management
- In-context domain documentation
- Hover text
- Object-based navigation for near real-time performance monitoring

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 role 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.

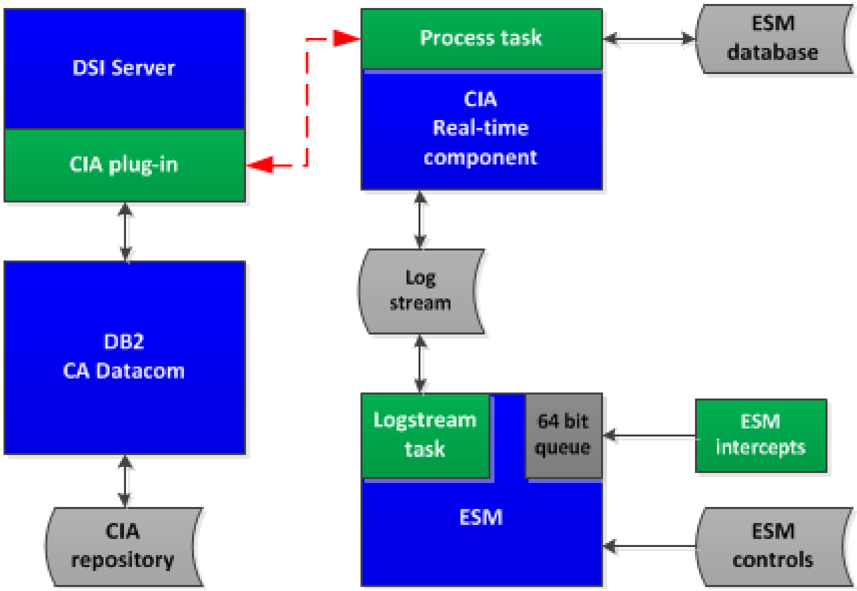
Note: The CIA real-time feature is available only when CA Chorus is installed at your site. When the CIA real-time feature is enabled, it performs an LMP check for the CA Chorus LMP key. Without the key, the CIA real-time feature cannot be enabled.

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.



CIA Real-Time Implementation Checklist

The following checklist is available to assist as you implement and configure the CIA Real-Time component.

Implement the CIA Real-Time Feature

Perform the following steps to implement the CIA real-time feature.

- Define the CIA repository for CA Datacom or DB2 (see page 137).
- Configure CA DSI Server for CIA real-time (see page 140)
  - Manually edit the dsi.conf configuration file using oedit or vi editor.
  - For DB2 CIA Security Repository usage - Replace the *ssid* with the DB2 subsystem name or group attachment name that the CIA real-time plugin connects.
  - For CA Datacom CIA Security Repository usage - Replace the *ssid* with the CA Datacom MUF that the CIA real-time plugin connects.
- Begin CIA real-time recording (see page 141).
  - Define the CIA real-time feature logstream.
  - Modify the CA Top Secret control options to enable recording of update requests to the CIA logstream.

- Load the CIA repository (see page 144).
  - Unload the security product database information on a z/OS image containing the security product database.
  - Load the security information into the CIA repository on the z/OS image that contains the CIA repository.

Configure the CIA Real-Time Component

Perform the following steps to configure the CIA real-time component.

- Define the CIA real-time component options. (Optional) (see page 146)
  - Copy data set member CIAPARMS in CAI.CAKOJCL0 into the procedure or parameter library that is designated according to your installation standards.
  - Edit data set member CIAPARMS to modify the CIA real-time component options to conform to your installation standards.
- Allocate the CIASTATS DD output data set. (Optional) (see page 147)
  - Check if this data set already exists. If it does not, edit the CIARTALC job in CAI.CAKOJCL0 to conform to your installation standards.
  - Submit the CIARTALC job.
  - Verify that the CIASTATS DD was successfully created.
- Allocate the CIAJRNL DD output data set. (Optional) (see page 147)
  - Check if this data set already exists. If it does not, edit the CIARTALC job in CAI.CAKOJCL0 to conform to your installation standards.
  - Submit the CIARTALC job.
  - Verify that the CIAJRNL DD data set was successfully created.
- Define the CIA Real-Time component (see page 148).
  - Copy the sample CIARTUPD procedure from the CAI.CAKOJCL0 installation data set to a procedure library in each z/OS system where the CIA real-time component will be executed.
  - Edit the CIARTUPD procedure.

Create the CIA Real-time Component Security Definition (see page 149)

Create the CA Top Secret security environment required for the CIA real-time component. Modify and run the CIARTTSS sample job.

Start and Stop the CIA Real-Time Component

Perform the following steps to start and stop the CIA Real-Time component.

- Automatically start during CA Top Secret initialization (see page 151).
  - Specify START on the CIAAUTO control option.
- Start with a console command (see page 151).
  - Issue the S CIARTUPD command at the console.
- Stop the CIA real-time component (see page 152).
  - Issue the P CIARTUPD command at the console.

Control and Modify the CIA Real-Time Component

Perform the following step to control the execution of the CIA real-time component address space.

- Issue the F CIARTUPD command at the console. (see page 152)

CIA Real-Time Component Prerequisites

The CIA real-time component requires the following to function:

- CA Top Secret r15 with the latest maintenance. For information about installing CA Top Secret, see the CA Top Secret *Installation Guide*.
- CA DSI Server r15 with the latest maintenance. For information about installing and configuring CA DSI Server, see the CA DSI Server *Installation Guide*.
- CA Chorus for Security and Compliance Management with the latest maintenance. For information about installing and configuring CA Chorus for Security and Compliance Management, see the CA Chorus Installation Guide.
- CA Chorus LMP key must be available on every z/OS image where the CIA real-time feature is enabled.

Implement the CIA Real-Time Feature

The following steps describe how to implement the CIA real-time feature:

- Define the CIA repository (see page 137)
- Configure CA DSI Server for CIA Real-Time (see page 140)
- Begin CIA Real-Time Recording
- Load the CIA Repository
- Implement the CIA Real-Time Component

Define the CIA Repository for CA Datacom

Perform the following steps on the z/OS image where the CA Chorus CIA repository resides. Most of these tasks are part of any CIA implementation.

1. Select the z/OS image that hosts the CA Chorus CIA repository.

   The CA Chorus CIA repository resides in a CA Datacom MUF on a single z/OS image. This repository can contain the security information from multiple security databases across your enterprise. The 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

2. Create the CA Datacom MUF that hosts the CA Chorus CIA repository.

   This step is a normal part of any CIA implementation. The considerations for selecting or creating the CIA subsystem that hosts the CIA repository are described in Create the CA Datacom MUF.

Define the CIA Repository for DB2

Perform the following steps on the z/OS image where the CA Chorus CIA repository resides.

1. Select the z/OS image that hosts the CA Chorus CIA repository.

   The CA Chorus CIA repository resides in a DB2 subsystem on a single z/OS image. This repository can contain the security information from multiple security databases across your enterprise. The 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 DB2 subsystem
   - performance profile with sufficient resources

2. Select or define the DB2 subsystem that hosts the CA Chorus CIA repository.

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

3. Define the CIA repository.

4. Set up the Workload Manager and Resource Recovery Attach Facility environments.

   The compliance reports execute a set of CIA service functions to retrieve information from the CIA repository. The CIA user-defined functions run in a Workload Manager (WLM) environment together with the Resource Recovery Attach Facility (RRSAF).

   Operating environment setup is required for running user-defined functions and stored procedures in CIA. If you have not set up your CIA environment to use WLM-established stored procedure address spaces, see the *IBM Redbook, "DB2 for z/OS Stored Procedures: Through the CALL and Beyond"* for direction on setting up WLM and RRSAF for this purpose. We recommend that you set up a separate WLM environment for the CIA service functions.

5. Define the CIA service functions.

   Choose the following option based on your site:

   CA ACF2

   Perform the following steps to define the service functions to the target DB2 subsystem.

   - Edit the CIAFUNC job in CAI.CAX1JCL0.

     Modify it to conform to your installation standards, and direct it to the target CIA subsystem.

   - Submit the job.

     The job runs and completes.

   - Verify the output of the CIAFUNC job.

     The CIA functions are defined.

   CA Top Secret

   - Edit the CIAFUNC job in TSS.SAMPJCL.

     Modify it to conform to your installation standards, and direct it to the target CIA subsystem.

   - Submit the job.

     The service functions are defined to the specified DB2 subsystem.

   - Verify the output of the CIAFUNC

     The CIA functions are defined.

6. Before the CIA service functions can be executed, bind the application packages that correspond to the service functions in the target CIA subsystem with the security repository.

   Choose the following option based on your site:

   CA ACF2

   - Edit the CIABIND job in CAI.CAX1JCL0.

     Modify it to conform to your installation standards and direct it to the target CIA subsystem.

   - Submit the job.

     The job runs and completes.

   - Verify the output of the CIABIND job.

     The DB2 packages are bound.

7. 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.

   Choose the following option based on your site:

   CA Top Secret

   - Edit the CIALINK job in CAI.CAX1JCL0.

     Modify it to conform to your installation standards, and direct it to the target DB2 subsystem.

   - Submit the job.

     The job runs and completes.

   - Verify the output of the CIALINK job.

     The CIA modules are linked

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.

The following configures the CA DSI Server for use with CIA real-time updates. Add the lines only if you are configuring this CA DSI Server to support CIA real-time updates to the CIA repository.

Note: Perform this step on the z/OS image where the CA Chorus CIA repository resides.

Follow these steps:

1. Manually edit the dsi.conf configuration file. For example, in USS use oedit or vi. In TSO use ishell or IPSF Edit, or use any other utility that can edit an HFS file. The dsi.conf file can be found in the directory that CA DSI Server was installed. Select the appropriate lines based on whether you are using DB2 or CA Datacom/AD, and add them to the end of the file.

   For DB2:

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

   Replace *ssid* with the CIA DB2 subsystem name or group attachment name where the CIA real-time plug-in connects.

   Note: 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.

For CA Datacom/AD:

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

Replace database-MUF-name with the name of the CA Datacom/AD MUF where the CIA real-time plug-in connects. CA Datacom/AD displays this value in the joblog at MUF statup in MUFNAME=.

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

For example:

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

Note: Enter all fields in uppercase.

2. Choose the following options based on your site:

   - For DB2 CIA Security Repository, replace *ssid* with the CIA subsystem name or group attachment name that the CIA real-time plugin connects.
   - For CA Datacom/AD CIA Security Repository, replace *mufname* with the CA Datacom/AD MUF that the CIA real-time plugin connects.

   Note: Enter all fields in uppercase.

   Important! Assign the DSI authorization to access the CA Datacom/AD or DB2 database plan. For authorization examples, see the DSICIA job in the CDT9JCL data set.

Begin CIA Real-Time Recording

Perform these 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 signon 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.

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

1. Define the CIA real-time feature 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.

Modify and run the CIALOGST sample job to define the CIA real-time feature logstream.

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 which 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 where this will 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 make an evaluation of your network and system stability and the effort involved in reloading the CIA repository information. If the time involved in either of the situations described is greater than the size of the logstream allows, the logstream fills up and update requests will be 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. Since 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).

2. Modify the CA Top Secret control options to enable recording of update requests to 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. For more information about the CA Top Secret control options, see the CA Top Secret *Control Options Guide*.

   CIART(ACTIVE)

   Specifies that CA Top Secret is to begin recording to the CIA logstream.

   CIALOGNAME

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

   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.

Note: In order to specify the CA Top Secret control options, you must also provide the CIAHOST and CIAPORT values. For more information about these options, see CIA Real-Time Control Options.

Load the CIA Repository

These steps must be performed for each security product database whose information is required in the CA Chorus CIA repository. Most of these tasks are part of any CIA implementation.

Note: Before you perform the process of unloading and loading the security database information into the CIA repository, you must ensure that you have started recording the CIA real-time update events on all z/OS system images that share the security database. If the security database unload is performed before recording is started, you will miss events that update the security information after the unload but before the start of recording, and the information in the CIA repository will not be accurate.

1. On a z/OS image containing the security product database, unload the security product database information.

   This step is a normal part of any CIA implementation. For more information about unloading the security product database see the Unload the Security Information.

   Note: If the security product database is shared across multiple z/OS images, it must be unloaded from only one of the z/OS systems.

2. On the z/OS image that contains the CIA repository, load the security information into the CIA repository.

   This step is a normal part of any CIA implementation. For more information about loading the security information into the CIA repository, see the Load the Security Information.

Implement the CIA Real-Time Component

Perform this step 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.

The CIA real-time component is a started task address space that reads the update requests from the CIA logstream and communicates the changes to the CIA repository. For more information about the implementation process for the CIA real-time component, see the CIA Real-Time Component Implementation for CA ACF2 or CIA Real-Time Component Implementation for CA Top Secret.

CIA Real-Time Component Implementation

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 login and logoff 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.

The CIA real-time component is a started task address space. The address space that reads the update requests from the CIA logstream and communicates the changes to the CIA repository.

The process of implementing the CIA real-time component consists of the following:

- CIA real-time component configuration
  - (Optional) Define the CIA real-time component options
  - (Optional) Allocate the CIASTATS DD output data set
  - (Optional) Allocate the CIAJRNL DD output data set
  - Define the CIA real-time component started task procedure
- CIA real-time authorization
  - AP-authorize library CAI.CAKOLINK
  - Create a control ACID with the following:
    - Unscoped control authority (type SCA)
    - Administrative authorities of DATA(ALL), ACID(DEFNODES), RESOURCE(INFO), MISC5(DCLLIST), MISC8(LISTRDT, LISTSDT), and MISC9(MODE)
    - USS capabilities such as UID, GID or group, home directory, and login shell
    - DSN(TCPIP.) ACCESS(READ)

  Note: Sample JCL member CIARTTSS can be used to create the control acid needed to run CIA real-time.

  - Add the CIA real-time component started task procedure name to the Started Task Command (STC) record with an assignment to the newly created control ACID.
- CIA real-time control options

  Specify the options for the CIA real-time component in the CA Top Secret control options.

CIA Real-Time Component Configuration

Proper configuration of the CIA real-time component is required for processing security update events in real time and communicating them to the CIA repository.

The following steps are necessary to configure the CIA real-time component:

- (Optional) Define the CIA real-time component options
- (Optional) Allocate the CIASTATS DD output data set
- (Optional) Allocate the CIAJRNL DD output data set
- Define the CIA real-time component started task procedure

Define CIA Real-Time Component Options

You can use a set of CIA real-time component options to control execution of the CIA real-time component. Because they are optional and should be set only if directed by CA technical support, you can follow these steps and establish the options member for when it may be needed, or you can bypass the definition of options completely.

To define CIA real-time component options

1. Copy data set member CIAPARMS in CAI.CAK0JCL0 into the procedure or parameter library that is designated according to your installation standards. This member could be SYS1.PARMLIB, SYS1.PROCLIB, or another library that your installation uses.

   CIAPARMS is an optional data set member and contains the options used to control the start up and execution of the CIA real-time component.

2. Edit data set member CIAPARMS to modify the CIA real-time component options to conform to your installation standards. Begin each option in column one. An asterisk in column one denotes a comment.

   The CIAPARMS DD statement in the CIARTUPD started task procedure JCL must point to this data set member.

Sample CIA Real-Time CIAPARMS Member

The following is a sample of how CIA real-time component options are specified in the CIAPARMS data set member:

```
***   All options are currently entered as comments  ***
* GTRACE
* TRACESIZE=262144
```

CIA Real-Time Component Option Descriptions

The CIAPARMS member in CAI.CAKOJCL0 holds the options that control the startup and execution of the CIA real-time component. The following options are supported:

[GTRACE]

(Optional) Activates the general trace facility (GTF) 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'. If you do not specify a value for this option, GTF tracing will not be active at component initialization.

Note: We recommend not activating GTF tracing unless instructed to do so by CA Technical Support.

[TRACESIZE=262144|nnnnnnn]

(Optional) Specifies the size, in bytes, of the internal trace table. Any value entered not on a kilobyte boundary will be rounded to the next higher kilobyte. If you do not specify a value for this option, the default is used.

Range: 32768 to 1048576

Default: 262144 (256 Kilobytes)

Note: We recommend not specifying this option unless instructed to do so by CA Technical Support.

Allocate the CIASTATS DD Data Set

CIASTATS DD is an optional output data set, that records the results of STATUS console commands processed by the CIA real-time component.

To create the CIASTATS DD data set

1. Check if this data set already exists. If it does not, edit the CIARTALC job in CAI.CAK0JCL0 to conform to your installation standards.

   Follow the instructions in the job to modify its contents. This job allocates the CIASTATS DD data set. Estimate the amount of space required for the CIASTATS DD data set and modify the space parameter, as necessary.

2. Submit the CIARTALC job.

3. Verify that the CIASTATS DD data set was successfully created by checking the job output.

Allocate the CIAJRNL DD Data Set

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 wrap-around data set.

Important! Size the data set correctly at creation so that required entries are not lost.

To create the CIAJRNL DD data set

1. Check if this data set already exists. If it does not, edit the CIARTALC job in CAI.CAK0JCL0 to conform to your installation standards. Follow the instructions in the job for modifying it.

   This job allocates the CIAJRNL DD data set. Estimate the amount of space required for the CIAJRNL DD data set and modify the 'BLOCKS=' and space parameter, as necessary.

2. Submit the CIARTALC job.

3. Verify that the CIAJRNL DD data set was 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.

1. Copy the sample CIARTUPD procedure from the CAI.CAK0JCL0 installation data set to a procedure library in each z/OS system where the CIA real-time component will be 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.

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.

CIA Real-Time Component Security Definitions

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

CIA Real-Time Control Options for 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.

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

CIAAUTO

Specifies whether CA Top Secret will automatically start the CIA real-time component started task during CA Top Secret initialization. For more information, see Automatically Start 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. For more information, see Begin CIA Real-Time Recording.

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. For more information, see Begin CIA Real-Time Recording.

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. Automatically Start During CA Top Secret Initialization.

CIART

Specifies whether the CIA real-time feature is active. For more information, see Start with a Console Command.

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. For more information about the CIA SYSID value, see Unload the Security Information.

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.

Start and Stop the CIA Real-Time Component

After completing the configuration, authorization, and control option 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 CA Top Secret initialization (see page 151)
- Start with a console command (see page 151)
- Stop the CIA Real-Time Component (see page 152)

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

Automatically Start During CA Top Secret Initialization

You can use CA Top Secret control options to automatically start the CIA real-time component started task as part of the CA Top Secret initialization.

To automatically start the CIA real-time component, specify START on the CIAAUTO control option. When START is specified, the CIA real-time component started task will be automatically started during of CA Top Secret initialization. The default is NOSTART.

Note: If you changed the name of the procedure you must also update the CIAPROCNAME control option so CA Top Secret knows which procedure to start.

Start with a Console Command

You can 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

Command	Operand	Description
	,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.

Journaling the Error Status of CIA Update Requests

You can view the completion status of requests that failed to update the CIA repository in an optional journal file that was configured before the component was started.

To view the completion status of failed events to a file

1. Allocate the CIAJRNL DD output data set.
2. Specify the name of the allocated data set in the CIAJRNL DD statement of the CIARTUPD procedure JCL.

Sample Journal Error Status Output

The following is a sample of the completion status for a failed update request that was journaled:

```
2010320 115433 Event:  ADDTO Profile Admin/User: SCAHP1   Jobname: SCAHP1    Source: A11L904
2010320 115433 Result: FAIL  Date/Time: 03/08/2011  10:13:12.15  Sysplex:          Sysid: xxxx
2010320 115433   Object: PROF001
2010320 115433   CIA0248E Error from call to DSI
```

CIA Real-Time Component Tracing

You can write trace entries to the active trace file for the purpose of capturing component diagnostic information.

Note: We recommend that you do not activate GTF tracing unless instructed to do so by CA Technical Support.

Write CIA Real-Time Component Trace Entries to GTF

The GTRACE command activates the general trace facility (GTF) 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'.

To write trace entries to the active trace file, Issue the following console command:

```
F CIARTUPD,GTRACE
```

Stop Writing CIA Real-Time Component Trace Entries to GTF

The NOGTRACE command deactivates the GTF option. Trace entries are no longer written to the trace file.

To stop writing trace entries to the active trace file, issue the following console command:

```
F CIARTUPD,NOGTRACE
```

Recover the CIA Real-Time Component

CIA real-time component address space recovery processing generates system dump requests as appropriate.

To recover the CIA real-time component, save any system dumps that are generated and the associated job logs and job output.

Note: For assistance, contact CA Technical Support at http://ca.com/support.

Resynchronizing the CIA Repository Information

A failure in the CIA real-time processing can cause the information in the CIA repository to no longer accurately reflect the information in the corresponding security product database. Some of the events that can cause this to occur are:

1. If the CIA real-time feature is disabled on one or more of the z/OS system images that share the security database, update events that change the security information are not recorded and communicated to the CIA repository.
2. If a problem occurs with the CIA logstream that causes it to become full before events can be deleted, update events that change the security information cannot be recorded and communicated to the CIA repository.

Regardless of the cause, after the information in the CIA repository becomes inaccurate, a procedure must be followed to reestablish the security information in the CIA repository.

If the CIA repository contains the information from multiple security database images, the information from only one of the security databases is likely to be inaccurate. This procedure reestablishes the security information from that single security database image, while leaving the rest of the CIA repository intact.

Resynchronization Checklist

Perform the following steps to resynchronize the CIA repository.

- Stop the CIA real-time process
  - Stop the CIA real-time component address space.
  - Stop the recording of CIA update events.
- Delete the CIA repository information
  - If the CIA repository resides in DB2, modify and execute the CIADELSI member in the sample JCL data set to delete the old information for the security database image.
  - If the CIA repository resides in CA Datacom/AD, modify and execute the CIADELSC member in the sample JCL data set to delete the old information for the security database image.

- Restart CIA Real-Time Recording
  - Delete and redefine the CIA logstream.
  - Start the recording of CIA update events.
- Reload the CIA Repository Information
  - Unload the security database information.
  - Reload the security database information into the CIA repository.
- Restart the CIA Real-Time Component
  - Start the CIA real-time component

Stop the CIA Real-Time Process

Perform these steps on every z/OS image that shares the security database whose information is being re-synchronized. Before the security information can be re-established, you must stop the CIA real-time processes that are updating that information.

1. Stop the CIA real-time component.

   On each of the z/OS images that share the security database, stop the CIA real-time component address space.

   For more information about commands to stop the CIA real-time component, see Stop the CIA Real-Time Component (see page 152).

2. Stop the recording of CIA update events.

   On each of the z/OS images that share the security database, stop the recording of CIA update events into the CIA logstream. Issue the CA Top Secret command to modify the CIART control option to INACTIVE.

Delete the CIA Repository Information

Perform this step on the z/OS image that contains the CIA repository. Before the security information can be reestablished, delete the old information for the security database image.

If the CIA repository resides in DB2, modify and execute the CIADELSI member in the sample JCL data set to delete the old information for the security database image. Detailed information about how to configure the job is contained in the comment prologue of the sample job.

If the CIA repository resides in CA Datacom/AD, modify and execute the CIADELSC member in the sample JCL data set to delete the old information for the security database image. Detailed information on how to configure the job is contained in the comment prologue of the sample job.

Restart CIA Real-Time Recording

Perform these steps on every z/OS image that shares the security database whose information is being re-synchronized in the CA Chorus CIA repository. Many of these tasks mirror the same process that was used in the initial CIA real-time implementation, and the detailed instructions for the tasks refer to the appropriate section of this chapter that describes the task.

1. Delete and redefine the CIA logstream.

   To re-initialize the CIA logstream, you must delete and redefine it.

   For more information about deleting and defined the CIA logstream, see Begin CIA Real-time Recording. (see page 141)

2. Start the recording of CIA update events.

   For more information about starting the recording of CIA update events, see Begin CIA Real-time Recording (see page 141).

Reload the CIA Repository Information

Perform these steps for the security product database whose information is being re-synchronized in the CA Chorus CIA repository. These tasks are part of any CIA implementation.

1. Unload the security database information.

   On a z/OS image containing the security product database, unload the security product database information.

   This step is a normal part of any CIA implementation. For more information about unloading the security product database, see Unload the Security Information.

   Note: If the security product database is shared across multiple z/OS images, it must be unloaded from only one of the z/OS systems.

2. Reload the security database information into the CIA repository.

   On the z/OS image that contains the CIA repository, load the security information into the CIA repository.

   This step is a normal part of any CIA implementation. For more information about loading the security information into the CIA repository, see Load the Security Information.

Restart the CIA Real-Time Component

Perform this on every z/OS image that shares the security database whose information is being re-synchronized.

Start the CIA real-time component

On each z/OS image that shares the security product database, start the CIA real-time component. For more information about the commands to start the CIA real-time component, see Start the CIA Real-Time Component (see page 151).

Index