CA Top Secret® Option for DB2

Product Guide

r1.3

Third Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA ACF2™
- CA Common Services
- CA CSM
- CA Top Secret® for z/OS (CA Top Secret)
- CA Top Secret® Option for DB2 (CA Top Secret Option for DB2)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Documentation Changes

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

- Consider the Effects of the Authorization Algorithm—added DB2 SYS (SYSDBADM).
- Special Authorization IDs—added paragraph about DB2 version 10.

Contents

Chapter 1: Introduction

This guide provides CA Top Secret Option for DB2 implementation considerations and describes a conversion utility that can assist in creating the same security structure that was implemented with DB2 security. The guide also provides troubleshooting information that can help identify and resolve problems.

This section contains the following topics:

About CA Top Secret Option for DB2

CA Top Secret Option for DB2 brings the powerful capabilities of CA Top Secret® for z/OS (CA Top Secret) to the DB2 environment. With a single-point centralized security strategy, it simplifies the complex process of managing access to critical DB2 resources, privileges and utilities. CA Top Secret Option for DB2 provides consistent security and logging, and easy auditing and reporting.

DB2 is IBM's strategic relational database management system. DB2 has its own internal security, where authorized DB2 administrators grant and revoke access to DB2 resources. CA Top Secret Option for DB2 replaces this native DB2 security with security for DB2 resources based on a security policy defined in resource permissions administered by a security administrator using the CA Top Secret Option for DB2 product.

The following are CA Top Secret Option for DB2 features at a glance:

- Provides powerful capabilities of CA Top Secret applied to DB2 environment
- Eliminates maintaining DB2 grant/revoke schemes and site written exits
- Simplified ownership principles reduce DB2 complexity
- Improved productivity with single-point centralized security
- Increased auditability with separation of security and database tasks

Disclaimer

All sample code provided with CA Top Secret Option for DB2 is intended for use as a reference aid only. No warranty of any kind is made to the completeness or correctness of sample code. CA Technologies, Inc. cannot be held responsible for any damages of any kind incurred by the client related to the use of any sample code.

Audience

The audience is primarily comprised of security administrators who have already installed DB2. In all probability, these security administrators will want to work closely with the DB2 DBAs to determine what DB2 databases, tables, plans, and so on, must be protected. This section details the responsibilities of certain team members involved in the implementation of security.

Security Administrator

The security administrator acts as the primary and central coordinator for security information and deals with all phases of implementing CA Top Secret Option for DB2. These responsibilities can include:

- Initial planning, which includes customizing the CA Top Secret Option for DB2 security environment
- Gradually implementing full security in FAIL mode
- Maintaining the Security file, reviewing incident and activity reports, and investigating suspicious events

A security administrator does not need previous programming experience, but it is helpful for this person to have some technical data processing knowledge.

The security administrator who uses CA Top Secret Option for DB2 should have a conceptual understanding of the vocabulary and procedures necessary to administer CA Top Secret Option for DB2. Most likely, this person will have hands-on experience in administering CA Top Secret in a z/OS (CA Top Secret) environment, using the TSS command or the administration panels.

DB2 Database Administrator

In general, DB2 DBAs design the databases and other components (tables, views, and so on) of the system. They create tables, determine which tables have indexes, and monitor the system's performance. They can be responsible for the operation, use, and maintenance of these components. If DBAs are already active in the data security area, they can often provide valuable input about current use and future data security needs. They should understand how security issues relate to their jobs and what their responsibilities are.

Systems Programmer

The systems programmer or the operations staff installs and applies maintenance to CA Top Secret Option for DB2. This person may also install and apply maintenance to DB2, or they might know nothing about DB2 at all. They should be familiar with the operating system, JES, SYSGENs, and related areas.

Applications Programmer

The applications programmer develops and tests DB2 application programs. They may create tables with test data as part of their job.

Why Do I Need CA Top Secret Option for DB2?

Databases are an integral part of your data processing environment. It is becoming more and more imperative that the administration and monitoring of database security are not separated from your day-to-day data security standards and procedures.

CA Top Secret Option for DB2 provides a single architecture from which you can control and monitor security- and audit-related events across your entire data processing environment. This DB2 product is another illustration of our commitment to develop integrated system software.

The following section describes some of the benefits derived from using CA Top Secret Option for DB2.

What Are Some of the Benefits?

The control of DB2 resources is accomplished using standard CA Top Secret methods. All DB2 resources have full scope checking and administrative authority support, which eliminates the need for secondary authorization IDs, and the cascading revoke problems. The direct benefits of CA Top Secret Option for DB2 are as follows:

- The DB2 resources are easily administered with the TSS command or the administration panels.
- In CA Top Secret Option for DB2, the concept of ownership through the creation of an object is eliminated. Instead, all DB2-related resources are preferably owned by a department and their use is authorized to users with appropriate privileges, and optional access controls, such as time of day, day of week, and so on.
- With CA Top Secret Option for DB2 you do not need secondary authorization IDs. In fact, they can obscure the lines of individual accountability.
- The elimination of the cascading REVOKE effect makes secondary authorization IDs somewhat unnecessary. Due to this elimination, it is easier for security administrators to control and manage these DB2-related resources and authorities.
- Support and security exist for all categories of DB2 privileges and authorities. Because the SYSADM authority has complete control over most DB2 resources, you should carefully limit and monitor its use as you would an MSCA.
- There are discrete checks with unique class names identifying the type of function secured.
- Specific class names permit matching of relationships with existing DB2 controls.
- Access levels are supported as applicable to each function.
- All auditing and violation activity within DB2 is recorded to SMF and/or the Audit/Tracking File. All current facilities for reporting, including the online TSSTRACK reporting utility, are supported.

What Terms Do I Need To Know?

Security administrators who wish to know something about native DB2 security should use the following terms as a primer in understanding the basic concepts. The terms are divided into two groups: *general terms* and *resource terms.*

General Terms

There are many terms used within the native DB2 environment. The following list provides the terms that are used throughout the subsequent chapters of this guide.

SQL

A Structured Query Language that can be used within DB2 to access data and to control access to resources through GRANT and REVOKE statements.

Process

A term used for a unit that has the same basic properties in every environment but depends on the environment. It involves the execution of one or more programs, and is the unit that contains allocated resources. The execution of an SQL statement is always associated with some process.

Owner

The primary owner of a DB2 object is the ID recorded in the CREATOR column of the relevant Catalog table.

Object

Anything that can be created or manipulated with SQL, such as: databases, table spaces, tables, views, or indexes. In CA Top Secret Option for DB2 these objects are also known as resources.

Primary authorization ID

This represents a user during a process to perform a DB2 operation. The primary authorization ID is also the user's original authorization ID, unless an exit changes it.

Secondary Authorization Ids

This represents an optional ID, which can hold additional privileges available to a process.

Current SQL ID

This is the current authorization ID of the user for those commands or statements where composite privileges are not used. The term “composite privileges” means that the execution of an SQL statement can be based on the privileges of more than one authorization ID of the process.

Explicit privilege

A specific privilege given to a process by execution of a GRANT statement.

Implicit privilege

A privilege which is not the result of any GRANT statement. The user has an implicit privilege as the owner of an object.

Resource Terms

The following are the types of objects or resources that must be controlled in DB2:

System Privilege

Represents resources that are not directly related to a table, database, etc., but rather represent the authority to perform a given function. Some examples are the ability to stop and start databases, run traces, issue display commands, and so on.

Database

Represents a logical collection of tables, table spaces and indexes. DB2 groups these objects into a database to let you control access to these objects as a single unit. Different types of access can be granted to a database in native DB2. CA Top Secret Option for DB2 also provides for these same types of access in its implementation. Some examples are the ability to create a table space in a given database, image-copy that database for backup, recover the database, etc.

Table Space

Represents a physical collection of tables, and is actually represented on DASD as a VSAM Linear Data Set.

Table/View

A table represents the actual collection of rows and columns of data. A view represents a logical look at a table or tables, and is presented to the DB2 interface *exactly* the same as a table.

Different types of access are allowed, ranging from read-only access (SELECT) through the various update requests (DELETE, INSERT, and so on.). In addition, for UPDATE requests or referential constraints, access to tables and views can be provided down to the column level.

Plan

Represents what DB2 uses to process the SQL statements that are embedded in a program. With plans, there are two types of access: BIND and EXECUTE.

Package

Enables you to break a plan down into manageable parts. A package represents the SQL statements from a single program and can be shared across applications.

Collections

Represents one or more packages grouped together under a collection-id.

Storage Group

Represents a collection of DASD volumes that DB2 can use to dynamically allocate table spaces.

Buffer Pool

Represents main storage reserved to satisfy the buffering requirements of table spaces.

Functions

A function is similar to a subprogram that can be used in an SQL request to let you manipulate data directly in the SQL request.

Stored Procedures

Stored procedures are compiled programs (stored at a local or remote DB2 server) that can be invoked by a DB2 client with the SQL CALL statement.

Schemas

When you create functions, stored procedures, distinct types, and JAR files, you can associate them with a schema. A schema is a logical grouping of these resources, and like collections, cannot be owned.

Distinct Types

Distinct types are user-defined data types that are used to describe what input and output data looks like. One of the reasons for using distinct types is that you can control what functions or procedures can use a distinct type to ensure that data is being processed correctly.

JAR Files

Java archive files (JAR files) are files that contain a group of Java classes that can be used in Java applications. JAR files are available beginning with DB2 Release 7.1.

Sequences

A sequence is a user-defined object that is used to create a sequence of numerical values in table data, according to the specifications in the sequence definition.

Roles

A role is very similar to a secondary authid. It is an alternate authid that can be assigned to a user when the user is accessing DB2 via a connection defined as a trusted context. Roles are available beginning with DB2 Version 9.1.

Trusted context

A trusted context is a security entity defined in a DB2 subsystem that identifies a connection to the DB2 subsystem with specific attributes. When a connection is made with those attributes, other attributes defined in the trusted context will also apply to the connection. Trusted contexts are available beginning with DB2 Version 9.1.

Command Notation

Enter the following exactly as they appear in command descriptions:

Command Syntax	Explanation
UPPERCASE	Identifies commands, keywords, and keyword values, which must be coded exactly as shown.
underlining	Identifies command abbreviations. The underlined letters represent the minimum abbreviation.
Symbols	“” / * # () , must be coded exactly as shown.

The following clarify command syntax; do not type these as they appear:

Command Syntax	Explanation
Lowercase	Indicates keyword values which you must supply.
[ ]	Identifies optional keywords.
|	Separates alternative keywords or values; choose one.
Elipsis …	Means the preceding value might be repeated more than once.

Note the following sample commands:

```
TSS ADD(acid) DSNAME(oper,oper,oper...)
```

The minimum keyword abbreviation is DSN and you must supply a value for acid and oper (operand); there can be more than one value for oper which is separated by commas.

```
TSS ADD(acid) PASSWORD(pswrd[,0-255])
```

The minimum keyword abbreviation is PAS and you must supply a password. You can optionally enter an expiration interval. If you do not choose an interval, CA Top Secret Option for DB2 will default to the installation's setting for the PWEXP control option.

TSS PER(acid) MODE(FAIL|WARN|IMPL|DORM)

You must supply a value for acid and choose one of the following modes: FAIL, WARN, IMPL, DORM.

CA Services: Enabling Solutions Through Experience

When it comes to getting on the information fast track, CA Services can recommend and install a full suite of portal and knowledge management solutions to keep your business moving. And our associates offer the proprietary know-how on custom-fitting your enterprise for solutions ranging from life cycle management, data warehousing, and next-level business intelligence. Our experts will leave you with the technology and knowledge tools to fully collect, exploit, and leverage your data resources and applications.

CA Education Services

CA Technologies Global Education Services (CA Education) offerings include instructor-led and computer-based training, product certification programs, third-party education programs, distance learning, and software simulation. These services help to expand the knowledge base so you are better able to use our products more efficiently, contributing to your greater success. CA Education has been developed to assist today's technologists in everything from understanding product capabilities to implementation and quality performance.

Because the vast community of education seekers is varied, so too are our methods of instruction. CA Education is committed to provide a variety of alternatives to traditional instructor-led training, including synchronous and asynchronous distance learning, as well as Unicenter simulation.

For training that must be extended to a wider audience—for a fraction of the cost and logistical hassle of sending everybody away to a class—CA Education offers excellent distance learning options.

CA Technologies: The Software That Manages eBusiness

The next generation of eBusiness promises unlimited opportunities by leveraging existing business infrastructures and adopting new technologies. At the same time, extremely complicated management presents challenges—from managing the computing devices to integrating and managing the applications, data, and business processes within and across organizational boundaries. Look to CA for the answers.

CA has the solutions available to help eBusinesses address these important issues. Through industry-leading eBusiness Process Management, eBusiness Information Management, and eBusiness Infrastructure Management offerings, CA delivers the only comprehensive, state-of-the-art solutions, serving all stakeholders in this extended global economy.

For More Information

Numerous resources are available to you for additional information. The online help system at SupportConnect.ca.com offers procedural information and answers to any questions you may encounter.

Chapter 2: Implementation Considerations

This chapter describes decisions that you must make regarding implementing CA Top Secret Option for DB2. You might have already made many of these decisions when you installed and implemented CA Top Secret, or you might be in the process of making the decisions. This chapter helps you address the decisions from a DB2 perspective.

The following practices can help you successfully implement CA Top Secret Option for DB2:

- Organize and plan your implementation. This process requires you to:
  - Provide adequate training
  - Review security policy
  - Identify your operating environment
  - Select CA Top Secret Option for DB2 options
  - Evaluate who should get access to various resources
- Identify users based on primary and secondary authorization IDs
- Secure DB2 subsystems
- Secure DB2 resources (controllable objects and system privileges)

- Secure DB2 data sets and stand-alone utilities
- Secure DDF (if applicable)

This section contains the following topics:

Decide on Centralized or Decentralized Security

With native DB2 security, your site may not have a choice as to how you administer security. Because of the way DB2 is designed, your database administrators (DBAs) may be responsible for many of the functions normally performed by security administrators. With CA Top Secret Option for DB2, your site can decide whether the security functions and responsibilities for DB2 are centralized or decentralized. Whether CA Top Secret Option for DB2 administration is centralized or decentralized (and to what degree) depends on the size, structure, and unique needs of your site. You may want some DBAs to perform a subset of administrative functions or you may want your security department to handle all security concerns. Central security administrators can administer any CA Top Secret Option for DB2 access permissions while security administrators in a decentralized environment have a more limited jurisdiction over DB2 resources. Security administrators in a centralized environment have a broader scope of authority, while security administrators in a decentralized environment are given control over smaller groups of ACIDs (for example, an individual department). Decentralized administrators may also have different levels of administrative authority (granted via the TSS ADMIN command).

For more information about centralized vs. decentralized security, see the CA Top Secret *User Guide* and *Implementation* guides.

Appoint Your Implementation Team

The main function of the implementation team is to properly implement CA Top Secret Option for DB2 and related security systems and procedures. Their function is limited because most of the work occurs during the planning and implementation phases. If you created an implementation team (IT) to implement CA Top Secret, you may want to use this team to implement CA Top Secret Option for DB2. In addition to the current members, you will want to ask DB2 database administrators to join this team if they were not already included. Their participation and acceptance of CA Top Secret Option for DB2 is essential to successfully implementing CA Top Secret Option for DB2, because they play a critical role in creating and maintaining DB2 resources.

Plan and Coordinate Your Implementation Schedule

As the implementation plan takes shape, you should schedule all activities and events, and distribute schedules throughout the site to all key organizations. You should coordinate implementation timetables with related implementations of other system or product installations so they do not conflict.

Follow these steps to prepare to implement CA Top Secret Option for DB2:

- Ensure the key departments and personnel take an active role in the implementation plans. Everyone must support the implementation.
- Meet with other department managers to determine their concerns. Introduce an approach to address their concerns without compromising security.
- Observe other knowledgeable workers as they perform their functions. This can help lead to other improvements in securing resources that they use daily.
- Communicate the scope, impact, and requirements of the implementation plan to the entire organization.
- Design the CA Top Secret Option for DB2 installation and security implementation. Be sure to take into consideration the current data center standards, conventions, and procedures for testing and production turnover.
- Ensure that key personnel understand their roles and are available to support the implementation project.
- Plan for personnel vacations, holidays, and other staff outages.
- Secure management approval for the complete implementation plan, objectives, approach, and timetables.

Distribute Documentation

Determine which members of your implementation team (IT) require CA Top Secret Option for DB2 guides. Ensure that they also have the applicable CA Top Secret documentation. You may want to distribute CA Top Secret Option for DB2 and CA Top Secret guides to various groups as shown:

All IT members:

- CA Top Secret Option for DB2 *Administrator Guide*
- CA Top Secret *User Guide*
- CA Top Secret *Command Functions Guide*
- CA Top Secret *Report and Tracking Guide*

Systems Programming IT Member

- CA Top Secret Option for DB2 *Administrator Guide*
- CA Top Secret Option for DB2 *Installation Guide*
- CA Top Secret Option for DB2 *Product Guide*
- CA Top Secret Option for DB2 *Messages Guide*
- CA Top Secret *Planning Guide*
- CA Top Secret *Messages and Codes*
- CA Top Secret *Control Options*
- CA Top Secret *User Guide*
- CA Top Secret *Command Functions Guide*

You may want to distribute additional documentation during the latter phases of implementation. For example, you should provide your operations staff with a copy of the CA Top Secret Option for DB2 *Messages Guide* before the first test.

Provide Adequate Training

Although not necessary, we recommend that you send your key implementation team members to DB2 classes and to CA Top Secret for z/OS training classes. CA Education Services offers classes in various cities on a regular basis. They can also provide on-site training for your organization. For more information about CA Top Secret training classes, see http://esupport.ca.com/ and select CA Education.

Review and Tailor Security Policy

Members of IT should know the company data security goals and objectives before implementing CA Top Secret Option for DB2. Your IT members must evaluate the existing security policy of the organization and determine whether you want to modify your existing policy before you implement CA Top Secret Option for DB2. Identify any areas of the policy that are unclear or inappropriate. Keep in mind the modifications that your team wants to make as you plan to implement CA Top Secret Option for DB2 security in your data center.

Identify Current Security Standards

The first step in reviewing your security policy is to identify existing site security policies or standards. Because not every site has a formal security policy, start by identifying what has already been protected. Then, based on the implementation plan, identify the changes you must make in your current security policy. Note the differences in policy or functions of the features. During the implementation of CA Top Secret Option for DB2, you can change anything that you did not implement in CA Top Secret the way you originally wanted. Communicate any necessary changes to the user community by publishing a new security policy.

Many factors influence a site's policies and objectives. These can include the following areas:

- Government regulations that can affect data security requirements at your site, such as the National Computer Security Center (NCSC) ratings, the Privacy Act, Foreign Corrupt Practices Act, Securities and Exchange Commission (SEC) and other agency regulations, and various other accounting and reporting requirements.
- Legal requirements, such as controls over Electronic Funds Transfers (EFT) and contractual agreements preventing the disclosure of information.
- Industry practices and agreements, as they relate to recognized standards of due care.
- The threats of sabotage, white-collar crime, and computer fraud.
- Good business practices, such as separation of function, clear lines of responsibility and authority, individual accountability, knowing what the control procedures are and that they are in place, knowing who has access to assets and records and controlling this access, and various auditing considerations.
- Existing corporate policies that relate to computer assets such as data security, access control, and auditing computer control.
- Impact on the user community, such as decisions that relate to the degree of functional separation and the degree of centralization or decentralization in the administration of CA Top Secret Option for DB2 and related controls.
- Procedure enforcement needs, such as naming conventions for ACIDs and resource prefixing.

Tailor Your New Security Policy

After you evaluate existing security policies and standards, you must tailor your new security policy to accommodate DB2 requirements. If these policies and goals are not known or defined, the IT will find it difficult to choose appropriate CA Top Secret Option for DB2 options and to proceed quickly through CA Top Secret Option for DB2 implementation. Communicate the new policy to your user community to ensure that they know the new goals. You can use CA Top Secret Option for DB2 as a tool to implement security policies, automate policy enforcement, and help the company achieve its goals in relation to DB2 security.

As you begin tailoring the security policy, you must make decisions based on the following questions:

- What is the condition of my current security system?
- How do I want to secure development versus production systems?
- Do I want to centralize or decentralize my security administration?
- What role should DBAs play?
- How do I migrate an application from test to production? What issues should I consider?
- How much authority do I want to give the developers of applications?
- What resources do I want to audit?
- Which audit tools do I want to use?

Identify Your Operating Environment

To select the most appropriate options and to effectively use CA Top Secret Option for DB2 controls, first identify local conditions that you must consider, such as:

- Local naming conventions
- Existing security mechanisms
- Uniqueness of user identification
- Operating system configuration

Establish Local Naming Conventions

Determine existing (or desired) naming conventions for

- ACIDs for TSO, batch, IMS, CICS, and distributed users who access DB2
- Names of DB2 subsystems
- Names of DB2 resources (such as databases, tables, table spaces, and so on)

Standard naming conventions for ACIDs, DB2 subsystems, and DB2 resources simplify the task of writing CA Top Secret Option for DB2 PERMITs. CA Top Secret Option for DB2 provides an additional method—besides prefixing—for reducing the number of entries that must be made to secure an installation's DB2 resources. This method is masking (sometimes referred to as “patterning”). It can be used to group DB2 resources whose names share similar characteristics. These shared patterns can be used as the operands of the keywords in TSS entries.

CA Top Secret Option for DB2 provides five different masking techniques:

- Floating pattern
- Variable character substitution
- Index substitution
- Fixed position
- ACID substitution

For more information about the five different masking techniques, see the CA Top Secret *Command Functions Guide*.

Identify Existing Security Mechanisms

Identify all existing security mechanisms such as GRANT and REVOKE statements or security checks built into applications. Decide which ones to replace with CA Top Secret Option for DB2. Before you implement CA Top Secret Option for DB2, you may want to keep current DB2 security mechanisms active. Through the DB2FAC control option, you can activate or deactivate CA Top Secret Option for DB2 security on a subsystem-by-subsystem basis.

Note: You can use the conversion utility to analyze your current DB2 security. For more information about the conversion utility, see the “Conversion Utility” appendix.

Evaluate your site's use of the System Authorization Facility (SAF). While DB2 uses SAF to validate your connection to the DB2 subsystem, DB2 does not use SAF to validate access to any of the resources in DB2. CA Top Secret Option for DB2 provides you with a greater degree of control over your DB2 environment. It validates each user's access to each individual resource. You can instruct CA Top Secret Option for DB2 to use the following criteria to make access decisions:

- The name of the resource.
- The type of resource.
- The environment of the request.

These criteria may make use of SAF to validate access to the subsystem unnecessary.

Ensure Uniqueness of User Identifications

Identify all users and any individual or group IDs. Ensure that each system user is positively identified with a unique CA Top Secret ACID and a single password. Ensure that you create appropriate PROFILE ACIDs in place of each secondary authorization ID whenever possible.

Review Operating System Configuration

Ensure that your site has met the following requirements (see the section entitled System Requirements in the “Installation” chapter for DB2 for specific information about each of these requirements):

- DB2 requirements
- CA Top Secret Option for DB2 requirements
- CAIENF requirements

Evaluate Use of Exits

You may want to reevaluate your use of the IBM DSN3@SGN and DSN3@ATH exits that give users additional privileges through secondary IDs. The DSN3@SGN and DSN3@ATH exits associate secondary authorization IDs to primary authorization IDs. IBM supplies these as default and sample exits. CA Top Secret uses the sample exits provided by IBM. You may be able to use PROFILE ACIDs to completely eliminate the use of secondary authorization IDs. If you rely on PROFILE ACIDS instead of secondary IDs to determine a user's privileges, you do not need to remove these exits. You should, however, remove any of the CA Top Secret IBMGROUP resources associated with secondary IDs. For more information about replacing secondary authorization IDs with PROFILEs, see the “Evaluate Use of Secondary Authorization Ids” section.

Evaluate Who Should Get Access to What

CA Top Secret Option for DB2 permissions grant access to all DB2 resources, such as databases, tables, and system privileges. Before you can write and implement CA Top Secret Option for DB2 PERMITs, you must be a security administrator or be PERMITted authority through a TSS ADMIN command.

To make your CA Top Secret Option for DB2 permissions as effective as possible, answer these questions before you start writing the PERMITs:

- What are the names of the resources that I want to share?
- With what facility should a DB2 subsystem be associated?
- Should each DB2 subsystem be assigned its own facility or should they be grouped?
- Which users should be able to use system privileges and utilities and under which facility?

- Which ACIDs should own the resources (for example, divisions, departments)

  Note: It is strongly recommended that CA Top Secret ownership of a resource (via the TSS ADD command function) take place on a divisional or departmental level, rather than on an individual user level. Individual users within that department or division can then be granted access to those resources on an as-needed basis.

- What authorization ids should be used for qualifying DB2 tables?
- Which users should be able to change the PERMITs? Do I want to restrict any of these users?
- Who do I want to share resources with?
- Can I group and mask them?
- Should some users be privileged? Should these users be scoped?
- Should I trace access to a DB2 object? Should I trace a particular user's access to an object? Should I track use of a system privilege or utility?
- For resources that have the same name in multiple DB2 subsystems, should the user have the same privilege in all DB2 subsystems or should the privilege be restricted to specific DB2 subsystems?
- How do I want others to use the data? Should they be restricted in any way (such as to a column or to a certain function)?
- Should I determine certain time periods (shifts) when users can access the data?
- What privileges does DB2 require to access these resources?
- What table (database, and other) functions should users be permitted to access?
- Who will be creating DB2 resource definitions?
- Will users be utilizing static or dynamic SQL (for example, precompiled programs or ad hoc queries)?

After you answer these types of questions, you can begin to construct PERMITs.

We recommend that you use the conversion utility to create a set of general rules. Then you can edit these rules to be more specific. See the “Conversion Utility” chapter for more information about the conversion utility.

Determine Appropriate Security Mode

The mode used for specific DB2 resource checks defaults to the mode of the facility used for the DB2 subsystem, unless the mode is specified on a PERMIT. The facility is determined by the specification of the DB2FAC control option. Consider the following scenario:

- TSO facility in WARN mode
- CICSPROD facility in FAIL mode
- DB2PROD facility in FAIL mode
- DB2 DSNP subsystem associated with DB2PROD via DB2FAC control option

All security checks from TSO or CICSPROD accessing DB2 subsystem DSNP will occur in FAIL mode under the DB2PROD facility. Unless MODE is specified on the resource permission, the mode is determined by the DB2 facility.

CA Top Secret Option for DB2 supports all four security modes (DORMANT, WARN, IMPLEMENT, FAIL) for DB2 resource protection.

Identify Users

Evaluate ACID Construction

In CA Top Secret Option for DB2, users are identified by their ACIDs. Each user must have an ACID and, in most cases, a password. In addition to individual user ACIDs, there are also ACIDs representing departments, divisions, and zones. The administrator for each of these divisions is called a control ACID and these ACIDs are known by the following names: DCA (for departments), VCA (for divisions), ZCA (for zones), SCA (for the entire installation) and MSCA (the master security control ACID). The LSCA is the only control ACID with a variable scope. He or she can administer zones, ZCAs or other LSCAs.

Profile ACIDs are used in a manner similar to DB2 secondary authorization ids. User attributes or resource authorizations that apply to several users can be added to one Profile. Once that Profile is added to a User, he or she acquires the authorizations or attributes granted to the Profile.

For more information about creating ACIDs, you can see your CA Top Secret *Command Functions Guide*. In deciding on ACID construction, you should consider how you will delegate resources as well as who will have access to those resources. In CA Top Secret Option for DB2, ownership of a resource (which implies ALL access to that resource) is not automatically granted to the creator. Instead, ownership for administration is designated via the TSS ADD command when the resource is identified to CA Top Secret. We highly recommend that you ADD resources to a department or division rather than ADDing that resource to a specific individual. Individual users can then be granted access on an as needed basis. For example, assuming you've already created a DB2DEPT ACID, to secure all tables beginning with the PAY* prefix, you would first issue the following command:

```
TSS ADD(DB2DEPT) DB2TABLE(PAY*)
```

To PERMIT individual ACIDs (both in and out of the DB2DEPT department) you would issue the following command:

```
TSS PER(useracid) DB2TABLE(PAY*) ACC(SELECT)
```

Evaluate Use of Secondary Authorization IDs

Secondary authorization IDs are IDs that users can associate with to gain additional privileges to DB2 resources. Users can exercise the privileges of a secondary ID by associating with it through an exit. Some of the reasons IBM created secondary IDs are to overcome the cascade effect and improve the ownership of DB2 objects. The cascade effect occurs when DB2 revokes a privilege from an ID that granted the privilege to other IDs. DB2 also revokes the privilege from the other IDs. The loss of privileges creates an administrative burden for the security administrator, because he must ensure that users have the appropriate privileges to do their jobs. Secondary IDs can create a cushion against this type of effect because they typically are not granted the WITH GRANT OPTION and cannot grant privileges to another ID.

Secondary IDs also address the problem of managing ownership of DB2 objects. When a user is terminated or transferred, the security administrator must revoke his privileges and grant them to another user. This can create administrative overhead and result in the cascade effect. With secondary authorization IDs, the security administrator can grant these privileges to a secondary ID instead. The user then can associate with the secondary ID and exercise the privileges it has. Through the exits, the security administrators must update only a list of who can associate with each secondary ID when a user is transferred or terminated.

If you use secondary IDs for the above purposes, recognize that they can be difficult to maintain, can increase the complexity of managing DB2 security, and can create significant performance overhead. When DB2 checks a user's authorization, it checks every ID associated with that user until it finds one that is authorized. If users have multiple secondary IDs, this process can be time-consuming. If you use secondary IDs to ease administration or to avoid the cascade effect, you should consider using profile ACIDs in CA Top Secret Option for DB2 to accomplish the same results. Profile ACIDs let similar groups of users access resources in the same manner. For example, if all clerks in the Personnel department need access to the SALARY DB2 table, you could issue the following commands:

```
TSS CREATE(PERCLRK) NAME('DB2 Pers. Profile') TYPE(PROFILE)
   PASSWORD(NOPW) DEPT(PERSDEPT)

TSS PER(PERCLRK) DB2TABLE(SALARY.) ACC(SELECT)
```

Likewise, if all clerks in the Accounts Receivable department required access to the ACCOUNTS DB2 table, the following commands would be issued:

```
TSS CREATE (ARCLRK) NAME('Accts. Rec. Profile') TYPE(PROFILE)
   PASSWORD(NOPW) DEPT(ARDEPT)

TSS PER(ARCLRK) DB2TABLE(ACCOUNTS.) ACC(SELECT)
```

If clerks in either department needed to access additional resources, the administrator would only need to update the Profiles. He would not have to update each individual clerks' ACID.

Some sites, however, use secondary IDs for purposes other than resource ownership. For example, users running applications that refer to an unqualified table name can use different versions of the table by changing their current SQL ID to a different secondary ID. If your site uses secondary authorization IDs in such a case, you can continue to use them with CA Top Secret Option for DB2 via the IBMGROUP resource class.

Note: Instead of using SET CURRENT SQLID as a means of qualifying tables for different systems, if each system has its own set of plans or packages, you can use the OWNER or QUALIFIER parameters of the DB2 BIND command for the same purpose. This will eliminate the need to use secondary IDs for table qualification.

In CA Top Secret, the IBMGROUP resource class is analogous to a RACF group name. In order to use IBMGROUP you must:

- Create a user ACID for the secondary authorization id. For example:

  ```
  TSS CREATE(PAYROLL) NAME('Payroll 2nd id') TYPE(USER)
    PASSWORD(NOPW,0) DEPT(DB2DEPT)
  ```

- Establish ownership of the resource class IBMGROUP(PAYROLL). For example:

  ```
  TSS ADDTO(DB2DEPT) IBMGROUP(PAYROLL)
  ```

- PERMIT the ACID to access the appropriate DB2 resources. For example:

  ```
  TSS PERMIT(PAYROLL) DB2TABLE(PAYROLL.EMPLOYEE) ACCESS(SELECT)
  ```

- PERMIT other ACIDs to access that ACID using the IBMGROUP resource class. For example:

  ```
  TSS PER(USERFRED) IBMGROUP(PAYROLL)
  ```

Under CA Top Secret Option for DB2, however, we recommend using standard profile ACIDs rather than the IBMGROUP resource class or DB2 secondary authorization ids.

CA Top Secret returns to DB2 the names of all resources permitted to the user under the IBMGROUP resource class. This includes a search for the user record, all attached profiles to the user, and the ALL Record.

All additional access restrictions, such as time of day, day of week, ACTION keywords are honored on each TSS PERMIT command function. However, if USERA has been permitted IBMGROUP(PAYROLL) on MONDAY to FRIDAY from 9 a.m to 5 p.m., and the authorization exit in DB2 is driven on TUESDAY at 6 p.m., CA Top Secret does *not* return the IBMGROUP(PAYROLL) in the list of resource names to which USERA has been permitted.

In summary, you can replace secondary IDs with PROFILE ACIDs when:

- used for grouping permissions
- BIND OWNER or QUALIFIER parameters are used to provide the implicit qualifier for unqualified table names.

Consider the Effects of the Authorization Algorithm

When a user requests access to a particular DB2 resource, CA Top Secret Option for DB2 takes in the following considerations to determine if that user is authorized to that resource:

- Privileges that would grant access beginning with the most explicit. For example, to determine if USERFRED had BIND authority to the PAYINQ.PAYPRM01 package, CA Top Secret Option for DB2 would consider the following permissions:
  - DB2PKG(PAYINQ.PAYPGM01) ACC(BIND)
  - DB2COLL(PAYINQ) ACC(PACKADM)
  - DB2SYS(SYSDBADM)
  - DB2SYS(SYSCTRL)
  - DB2SYS(SYSADM)

  The first permission is the most explicit.
- Authorization ids associated with the user. They include:
  - Current SQLID - the first authorization checked.
  - Primary authorization id
  - Each secondary authorization id

Identify DB2 Subsystems

The DB2FAC control option in the CA Top Secret Parameter File is used to associate a DB2 subsystem with an CA Top Secret facility. This association is used by CA Top Secret Option for DB2 to determine whether to protect the DB2 subsystem when it is started and whether to restrict access to a resource in the DB2 subsystem. DB2TEST and DB2PROD are the two predefined facilities in CA Top Secret that can be used for this purpose. You can group multiple DB2 subsystems with a single facility or you can assign each DB2 subsystem to its own facility. In the later case, we recommend that you define a new facility for the DB2 subsystem and name the facility the same as the DB2 subsystem.

There are three steps to identifying the DB2 subsystems. They are:

- Set the DB2FAC control option
- Identify the DB2 started tasks to the CA Top Secret STC Record.
- Identify users who can connect to DB2 through the DB2 resource class.

Set DB2FAC Control Option

The following is a description of the DB2FAC control option. For a more detailed explanation of how control options operate in general, see the eTrust CA-Top Secret for z/OS *Control Options Guide*.

DB2FAC logically groups DB2 subsystems under different facility names. This controls via MODE, whether the resources in a DB2 subsystem are protected. The facility chosen further determines what the settings are for other facility control options (LOG, ABEND, NOABEND, etc.)

Format	Default	Entry Method
DB2FAC(ssid=facility)	None	All

where:

ssid

Identifies the name of the DB2 subsystem.

facility

Indicates the facility name to which the DB2 subsystem is associated.

The mode on the facility defined for the DB2 subsystem controls the protection of the DB2 subsystem resources. Specifying a non-DORMANT mode for the facility associated with the DB2 subsystem, will protect its resources. A mode of DORMANT, or no DB2FAC control option specification for a DB2 subsystem, indicates that CA Top Secret Option for DB2 will not protect the resources in the DB2 subsystem. The facility mode also determines the default mode for all CA Top Secret Option for DB2 resource checks to the DB2 subsystem.

The entry shown next indicates that DB2 subsystems DB2A and DB2B are grouped under DB2PROD, while DB2 subsystems DB2C and DB2D are under DB2TEST:

```
DB2FAC(DB2A=DB2PROD)
DB2FAC(DB2B=DB2PROD)
DB2FAC(DB2C=DB2TEST)
DB2FAC(DB2D=DB2TEST)
```

The entry shown next indicates that the subsystems identified to the DB2PROD facility are protected by CA Top Secret Option for DB2, while the subsystems identified to the DB2TEST facility are not protected by CA Top Secret Option for DB2:

```
FAC(DB2PROD=MODE=FAIL)
FAC(DB2TEST=MODE=DORMANT)
```

Identify and Secure DB2 Started Tasks

Each DB2 region begins its execution as a started task. Therefore, an CA Top Secret ACID must be associated with each DB2 region. This ACID must be able to access the STC facility and must be authorized to all data sets used within the region since these data sets are opened by DB2 itself. This ACID is referred to as the DB2 region control ACID. The ACID is associated with the region via the STC table.

After setting the DB2FAC control option, you must define the following DB2 started tasks to the CA Top Secret STC Record:

- xxxxMSTR
- xxxxDIST
- xxxxDBM1

(where xxxx = the four character subsystem id).

In addition, DB2 uses IMS Resource Lock Manager (IRLM) to manage the locking of DB2 resources. You specify the name of this started task during the DB2 install process.

For example, to secure the DSNXMSTR DB2 started task for the DSNX DB2 subsystem you would first create an ACID for that task:

```
TSS CREATE(DB2STC1) TYPE(USER) NAME('DB2 MSTR STC') DEPT(DB2DEPT)
  PASSWORD(NOPW,0) FAC(STC) NOVOLCHK NODSNCHK NORESCHK NOLCFCHK
  NOSUBCHK
```

Note: You can specify the NODSNCHK, NORESCHK, and NOLCFCHK attributes for the region control ACID. If you do not specify these attributes every resource and/or LCF-protected transaction ID will have to be permitted to the region control ACID.

After each region is associated with a particular ACID, the next step is to define the actual started task to the CA Top Secret STC table. This is done via the following syntax:

```
TSS ADD(STC) PROC(procname) ACID(regionacid)
```

For example, the command shown next will add the DSNXMSTR STC to the STC Record and associate it with the DB2STC1 ACID.

```
TSS ADD(STC) PROC(DSNXMSTR) ACID(DB2STC1)
```

Determine Access Authorizations to DB2 Subsystem

Access to specific DB2 subsystems is controlled outside of DB2. You do not signon to DB2; instead, DB2 calls the System Authorization Facility (SAF) when you connect to DB2.

The ACID associated with the DB2 connection request must be given the appropriate connection authorization via the **DB2** resource class keyword. The syntax is as follows:

```
  {(DSNR.ssss.BATCH)} for BATCH and TSO connections
  {(DSNR.ssss.DIST) } for Distributed Data Facility (DDF) connections
DB2 {(DSNR.ssss.MASS) } for IMS connections
  {(DSNR.ssss.SASS) } for CICS connections
ssss
```

Represents the subsystem name your site is using for DB2.

The ACID associated with a job is used to validate the connection for TSO and BATCH.

Individual user checking is not performed for IMS and CICS connections. Instead, the ACID associated with the IMS and CICS STCs or the associated MASTFAC ACID is used.

Identify DB2 Resources

DB2 resources can be broken down into two groups — controllable objects and system privileges. CA Top Secret Option for DB2 uses resource classes to protect these DB2 resources. In order to secure these resources you must:

- Identify them to CA Top Secret by ADDing them to a predefined DB2 user or department ACID. For example:

  ```
  TSS ADD(DB2DEPT) DB2TABLE(USRMIKE.RES)
  ```

- PERMIT these resources to individual users. For example:

  ```
  TSS PER(USER01) DB2TABLE(USRMIKE.RES) ACC(SELECT)
  ```

Evaluate Use of Default Protection (DEFPROT)

It is recommended that you assign the DEFPROT attribute to all DB2 resource classes. The DEFPROT attribute forces protection by default on all resources in a given resource class.

Issue the following command to add DEFPROT to a resource class:

```
TSS REPL(RDT) RESCLASS(DB2STOGP) ATTR(DEFPROT)
```

Member DB13RDT in the installation sample JCL library contains the commands for performing this administration.

Evaluate Use of RES Suboption

To protect DB2 resources in an online, multi-user facility (such as CICS), you must specify the RES suboption of the FACILITY control option for the facility you log onto. For example, to protect DB2 resources accessed from the CICSPROD facility, you would issue the following command:

```
TSS MODIFY FAC(CICSPROD=RES)
```

Evaluate Use of Additional Access Restrictions

In addition to specifying an access level for each of the DB2 resource objects (DB2SYS is used to control system privileges and does not have access levels), you can specify any of the following access restrictions for all of the DB2 resources:

EXPIRE

Limits the duration of the ACID's access to a particular resource. For example, if USRE01 needed temporary access to the “USRMIKE.RES” table for two weeks, the following command would be issued:

```
TSS PER(USER01) DB2TABLE(USRMIKE.RES) ACC(SELECT) FOR(14)
```

FACILITY

Allows the user access to the DB2 resources residing in a particular facility (i.e., DB2PROD, DB2TEST). For example, to allow USER01 access to the XYZ application plan only in the DB2PROD facility, the following command would be issued:

```
TSS PER(USER01) DB2PLAN(XYZ) ACC(EXECUTE) FAC(DB2PROD)
```

In a DB2 environment, it is likely that multiple DB2 subsystems will have resources with the same name. In fact, system privileges have the same resource name in all DB2 subsystems.

TIME/DAY

Limit access to certain days of the week, certain times of the day, or both. For example, to PERMIT USER03 to access the DSNP DB2 subsystem only on Mondays, Wednesdays and Fridays between the hours of 9 and 5, the following command would be issued:

```
TSS PER(USER03) DB2(DSNR.DSNP) DAYS(MON,WED,FRI) TIME(09,17)
```

ACTION

Specifies how CA Top Secret Option for DB2 will react to a request to access a particular resource. ACTIONS are divided into six types. They include:

- FAIL—Regardless of the mode the ACID is in, any attempts to access this resource are treated as though the ACID is in FAIL mode. Unauthorized access is failed. Ordinarily, if the user had been in WARN mode, he would have received messages upon attempting to access the resource but he would have succeeded in his attempt.
- AUDIT—The ACID is audited when this resource is accessed.
- NOTIFY—CA Top Secret Option for DB2 will notify the security console when the resource is accessed.
- EXIT—If the PERMIT is granted, CA Top Secret will issue the EXIT call to invoke the Installation Exit
- DENY—Used to deny access to resources that do not support access levels.
- ADMIN—ACTION(ADMIN) allows an administrator to PERMIT access to resources that are outside of his normal scope of authority. If an ACCESS level is not specified, the administrator is PERMITted to authorize the default access level associated with that resource class in the RDT.

For example, to indicate that an AUDIT record should be maintained of every time USER03 accesses the PAY001 application plan, the following command would be issued:

```
TSS PER(USER03) DB2PLAN(PAY001) ACC(EXECUTE) ACTION(AUDIT)
```

For more information about these access restrictions, see the CA Top Secret *Command Functions Guide*.

Using System Privileges

DB2SYS resources are global in nature — they represent a special type of permission and do not relate to a specific object. There is only one instance of the resource or permission type in the system, therefore it is recommended that the DB2SYS resources or permissions be owned by a corporate entity (such as a department). For example, to assign SYSADM privilege to the security department, the following command would be executed:

```
TSS ADD(SECDEPT) DB2SYS(SYSADM)
```

System privileges have the same resource name in all DB2 subsystems. Use the facility access control to restrict a system privilege for a user to a specific DB2 subsystem. For example, to assign SYSADM privilege to user JONES01 for DSNT subsystem which is associated with the DB2TEST facility, the following command would be executed:

```
TSS PER(JONES01) DB2SYS(SYSADM) FAC(DB2TEST)
```

In general, native DB2 system privileges have the same meaning in CA Top Secret Option for DB2. There are two exceptions — DB2SYS(CREDBA) and DB2SYS(CREDBC). In native DB2, the CREATEDBA privilege grants the user the explicit privilege to create databases and an implicit privilege of DBADM authority over those databases. CREATEDBC acts in the same manner, however, it only grants an implicit privilege of DBCTRL authority over the databases created by the user.

In CA Top Secret Option for DB2, the DB2SYS privileges of CREDBA and CREDBC both grant the explicit privilege to create databases. However, there are no implicit privilege of DBADM or DBCTRL for the created databases. Unlike DB2, the creator is NOT treated as the owner in CA Top Secret Option for DB2.

Explicit/Implicit Privileges and Authorization Hierarchy

DB2 privileges are bestowed in DB2 explicitly by issuing a GRANT statement, or implicitly every time a DB2 object is created.

In CA Top Secret Option for DB2, however, only explicit privileges are recognized. The creator of an object does not automatically gain privileges over the object.

CA Top Secret Option for DB2 supports the DB2 hierarchy of authorities. The significant difference between hierarchical authorities and standard privileges is that you can permit access to one DB2 object via a permission granted to another DB2 object. For example, the ALTER privilege for the PAYROLL.SALARY table could be given explicitly via the following command:

```
TSS PERMIT(JONES) DB2TABLE(PAYROLL.SALARY) ACC(ALTER)
```

Or implicitly through any of the following:

```
TSS PER(JONES) DB2DBASE(PAYROLL) ACC(DBADM)

TSS PER(JONES) DB2SYS(SYSDBADM)
TSS PER(JONES) DB2SYS(SYSCTRL)
TSS PER(JONES) DB2SYS(SYSADM)
```

Special Authorization IDs

As part of the DB2 installation, four special authorization IDs are defined to DB2 — two for install SYSADM and two for install SYSOPR. You have to CREATE an ACID for each of these IDs if you wish to use their authorities. At the very least, you will need to CREATE an ACID for one of the install SYSADM IDs. No other CA Top Secret Option for DB2 PERMITs will need to be issued.

Install SYSADM and install SYSOPR are extremely powerful authorities and should, therefore, be granted only with the highest consideration. You should consider associating them with an SCA or the MSCA for use during installation and maintenance. You might also want to add special controls, such as AUDIT, to these ACIDs.

In DB2 version 10 and above, two additional special authorization IDs are defined during DB2 installation. These authids are the install SECADM authids. In native DB2, these authids have the authority to perform the GRANTS and REVOKES of native DB2 security and to control security definitions such as row permissions and column masks. However, with CA Top Secret Option for DB2 these authids are not associated with the SECADM authority. The SECADM authority is controlled with a system authority permission just as other system privileges and authorities are controlled. The entity in the authority permission is SECADM.

Using BINDAGENT

Unlike other DB2SYS privileges that have global scope, BINDAGENT privilege only grants access authority for a specific owner. For example, to authorize USRFRED as the bind agent for USRJIM's packages, the following command would be issued:

```
TSS PER(USERFRED) DB2SYS(BINDAGENT.USERJIM)
```

This command allows USERFRED to BIND application plans and packages for USERJIM without having acquired access privilege for DB2 objects in those plans or packages. At BINDTIME, USERJIM's ACID is still checked for the appropriate authorizations.

Protect Table Columns

For table updates and referential constraints, you can permit access to the entire table or to selected columns of a table. For example, to give USRFRED UPDATE access to the BONUS column of the PAYROLL.SALARY table, you would issue the following command:

```
TSS PER(USRFRED) DB2TABLE(PAYROLL.SALARY.BONUS) ACC(UPDATE)
```

Identify and Secure DB2 Data Sets

Access to DB2 data sets takes place through the DB2 subsystem (i.e., through one of the DB2 started tasks) or through one of the DB2 stand-alone utilities (DSN1COPY, DSN1PRNT or DSN1LOGP).

Standard access to the DB2 data sets is granted by issuing a TSS PERMIT using the DSN resource class. For example, to authorize a user with an ACID of SYSADM1 to access all data sets with a high level qualifier of DSNX, the following command would be issued:

```
TSS PER(SYSADM1) DSN(DSNX.) ACC(ALL)
```

To require users to access the DB2 data sets via one of the DB2 stand-alone facilities, you would use the PRIVPGM keyword. For example:

```
TSS PER(DB2PROF1) DSN(DSNX.) PRIVPGM(DSN1LOGP)
```

Access to these data sets or utilities must be granted to the install SYSADM and install SYSOPR administrators.

Protect Distributed Data Facility (DDF) Resources

DB2 enables client applications that run in a remote environment to access data in a local DB2 server. It also enables local DB2 applications to access data at remote relational database systems.

You should associate the address space of the subsystem with a DB2 facility using MASTFAC. Each user will need to be granted access to this facility along with the appropriate DSNR.subsys.DIST connection resources.

The security package (for example, CA Top Secret, CA ACF2, RACF) that manages the subsystem on which the DB2 objects reside, determines what security restrictions will apply. For example, if subsystem A is the local subsystem and if the DB2 objects are maintained on subsystem B, access authorizations are determined by the security package in effect for system B.

Test PERMITs Using TSSSIM (optional)

The TSSSIM utility provides the ability to test permissions stored in the Security File without affecting the “real” production environment. Testing consists of invoking a simulated resource command for a specific resource. TSSSIM will report whether the currently active simulated ACID has access to that resource under the specified conditions. These conditions can include SVC-in-control, access level, privileged program and facility restrictions.

TSSSIM can also be used as a diagnostic tool in order to debug the Security File. For example, if a user has several Profiles attached to his ACID, it might be difficult to pinpoint the source of an access authorization or denial. By interpreting trace information generated by the security algorithm, TSSSIM can isolate the exact permission or ownership as well as the record (user, profile, ALL) in which the permission is contained.

TSSSIM can be executed under TSO, BATCH and Advantage™ CA Roscoe®. You should note, however, that when access to DB2 resources is tested, TSSSIM does not perform hierarchical checking. Access information extracted from TSSSIM is based on explicit PERMITs and ADDs for each resource. Implied or associated access to another, related resource, although valid in a PERMIT, is not taken into consideration by TSSSIM.

For more information about using the TSSSIM utility, see your CA Top Secret *Troubleshooting Guide*.

Chapter 3: Using the Conversion Utility

If you use native DB2 security, using the CA Top Secret Option for DB2 Conversion Utility simplifies the initial CA Top Secret Option for DB2 administration for DB2 resources. This utility procedure converts SQL GRANT entries, located in the DB2 catalog, into TSS ADDTO and TSS PERMIT commands. Note that, we recommend you run the conversion utility to create your first set of TSS commands for DB2 resource authorizations. These converted commands will provide a base for writing subsequent commands.

Once the process is underway, you should:

- Identify if certain key resources have been properly protected. This is done by reviewing the generated TSS ADDTO and TSS PERMIT commands.
- Review who should own the DB2 resources and whether each user who is granted access to those resources, should continue to have access, as well as a specific type of access.

Before running the conversion utility, ensure that the following procedures have been met:

- CA Top Secret Option for DB2 is installed
- The proper administrative authority has been assigned. Your scope must include the ACIDs that are to be converted.
- Create any new ACIDs for departments, profiles and users that you intend on giving ownership or permitting access to DB2 resources.
- Delete ACIDs for any secondary IDs that will no longer be used. This ensures that CA Top Secret Option for DB2 does not create valid ownership or permissions for IDs that you want to eliminate from your system.

To convert DB2 GRANTS to CA Top Secret Option for DB2 authorities, follow these steps:

- Allocate data sets for use by the conversion programs
- Unload the DB2 catalog GRANT data
- Convert the DB2 GRANT catalog entries into CA Top Secret Option for DB2 commands
- Customize the CA Top Secret Option for DB2 commands output file
- Execute the TSS commands

This section contains the following topics:

Step 1: Allocate Data Sets for the Conversion Programs

The CNVALLOC member allocates data sets used by the conversion programs. Edit the JCL to conform to your installation's standards. Depending on the amount of DB2 GRANT information in the DB2 catalog, you might have to increase the size of the SPACE parameters in the JCL. Submit the job and review the output.

Step 2: Unload the DB2 GRANT Data

The CNVGRANT member unloads the DB2 GRANT data from the DB2 catalog and saves it in a partitioned data set (PDS) for use by the conversion program in the next step. Edit the JCL to conform to your installation's standards. Submit the job and review the output. If the job fails because the output file is too small, restart the job after increasing the SPACE allocation in the allocation step.

Step 3: Convert the DB2 GRANT Catalog Entries into CA Top Secret Option for DB2 Commands

The CNV2TSS member converts the DB2 GRANT data from each of the PDS members created in the unload step. Edit the JCL to conform to your installation's standards. The ADD= keyword in the PARM field requires that you supply the name of the ACID that is assigned ownership of the DB2SYS resource authorities: SYSADM, SYSOPR, etc.. The FAC= keyword in the PARM field lets you specify the name of the facility to which the newly generated PERMIT statements are restricted. For example, if all of the converted GRANTs are to be restricted to the DB2PROD facility, you would code FAC=DB2PROD.

If the converted GRANTs are to be applied to ALL facilities, do not specify a value for the FAC= field, or omit the FAC= field entirely. Submit the job and review the output.

Step 4: Customize the CA Top Secret Option for DB2 Commands Output File

At this point, the TSS commands output file from Step 3 can be edited in order to assign ownership to validly existing departments and to change accesses. For example, to add date and time constraints on PERMIT commands or to change ACIDs that were used for secondary authorization IDs in native DB2 to validly existing profiles.

Step 5: Execute the TSS Commands

The CNVEXEC member executes the TSS commands using BATCH TMP. Edit the JCL to conform to your installation's standards. Submit the job and review the output. You might want to break this job up into smaller jobs for easier control and review.

Chapter 4: Troubleshooting

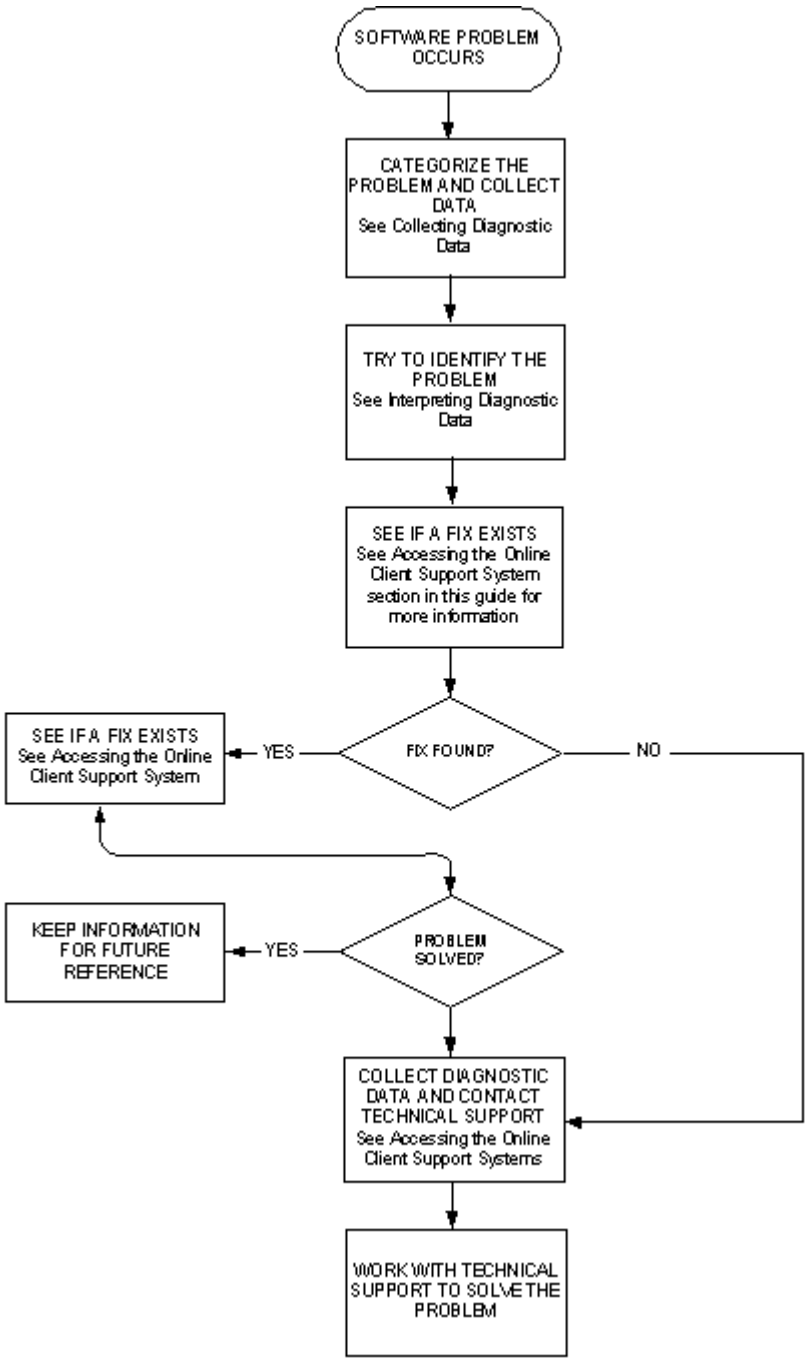
This chapter contains information about:

- Identifying and resolving problems
- Contacting CA Technologies Technical Support
- Receiving ongoing product releases and maintenance
- Requesting product enhancements

This section contains the following topics:

Diagnostic Procedures

See the following flowchart for a summary of the procedures you should follow if you have a problem with a CA Technologies software product. Each of these procedures is detailed in the following flowchart.



Collecting Diagnostic Data

In the following table, use the left column to categorize the problem your site has encountered. Then, follow the instructions in the corresponding right column to generate useful diagnostic data.

Type of Problem	Procedure
CAIENF	■ *CA Common Services Administrator Guide* and *Product Guide* ■ CAS9DB database utility LIST command output ■ Console messages ■ CAIENF operator command output ■ Output obtained from the ENF SVCDUMP or the ENF DUMP command.
CA Top Secret Option for DB2	■ Traces ■ TSS messages ■ Console messages ■ SYSLOG for violation messages ■ SECTRACE ■ CA Top Secret Option for DB2 trace ■ SVC dumps ■ User dumps ■ Output of TSS command

Interpreting Diagnostic Data

When you have collected the specified diagnostic data, write down your answers to the following questions:

1. What was the sequence of events prior to the error condition?
2. What circumstances existed when the problem occurred and what action did you take?
3. Has this situation occurred before? What was different then?
4. Did the problem occur after a particular PTF was applied or after a new release of the software was installed?
5. Have you recently installed a new release of the operating system?
6. Has the hardware configuration (tape drives, disk drives, and so forth) changed?

From your response to these questions and the diagnostic data, try to identify the cause and resolve the problem.

If you determine that the problem is a result of an error in a CA Technologies software product, you can use the CA Customer Service System (CSS) to see if a fix (APAR or PTF) or other solution to your problem has been published.

Accessing the Online Client Support Systems

For technical assistance, contact CA Technologies Technical Support at http://supportconnect.ca.com for a complete list of CA Technologies locations and telephone numbers. Technical support is available 24 hours a day, seven days a week.

Have the following information ready before contacting CA Technologies Technical Support:

- All the diagnostic information described in the Collecting Diagnostic Data section.
- Product name, release number, service pack, and operating system.
- Product name and release number of any other software you suspect is involved.
- Release level and PUTLEVEL of the operating system.
- Your name, telephone number and extension (if any).
- Your company name.
- Your site ID.

- A severity code. This is a number (from 1 to 4) that you assign to the problem. Use the following to determine the severity of the problem:
  - 1 =a “system down” or inoperative condition
  - 2 =a suspected high-impact condition associated with the product
  - 3 =a question concerning product performance or an intermittent low-impact condition associated with the product
  - 4 =a question concerning general product utilization or implementation

Tracing CA Top Secret Option for DB2 Authorization Calls

When CA Technologies Technical Support instructs you to, you can execute the CADB2TRC program to turn the internal diagnostic tracing for CA Top Secret Option for DB2 on or off. The diagnostic trace messages provide CA Technologies Technical Support with information regarding the DB2 authorization calls.

Use the following sample JCL to execute CADB2TRC:

```
//jobname JOB acct.info,'DIAG TRACE',CLASS=A,MSGCLASS=1
//CADB2TRC EXEC PGM=CADB2TRC,
//          PARM='TRACE=ON,TYPE=ALL,SUBSYS=DSNT'
```

The execute PARM for CADB2TRC indicates for which DB2 threads CA Top Secret Option for DB2 produces diagnostic trace messages. The following valid PARM keywords are described.

TRACE=ON|OFF|QUERY

The TRACE keyword is required with one of the following operands:

ON

Turns on diagnostic tracing.

OFF

Turns off diagnostic tracing.

QUERY

Produces a list of active traces.

TYPE=ALL|USER|JOB|CONNAME|CONTYPE

The TYPE keyword is required if you specify TRACE=ON|OFF, and must have one of the following operands:

ALL

The trace is for all threads.

USER

The trace is for a specific user(s).

JOB

The trace is for a specific job(s).

CONNAME

The trace is for a specific connection name(s).

CONTYPE

The trace is for a specific connection type(s).

SUBSYS=subsystemname

The SUBSYS= keyword is required, and has only one operand, subsystemname.

subsystemname

Indicates the explicit name of the DB2 subsystem CA Top Secret Option for DB2 is protecting for which you are requesting diagnostic trace messages. You *cannot* mask the subsystem name.

NAME=typename

The NAME keyword is required when you are also specifying the TYPE= keyword, and has only one operand, typename.

Typename

Indicates the name of the thread type to trace. You can specify the name with a mask as follows:

?—Matches any single character.

*—Matches all remaining characters, including null.

When you specify TYPE=USER, typename specifies the primary authorization ID to trace.

When you specify TYPE=JOB, typename specifies the name of a job to trace.

When you specify TYPE=CONNAME, typename specifies the connection name to trace (such as BATCH, TSO, DB2CALL). A connection name of SERVER is used for distributed calls when the remote system is not DB2.

When you specify TYPE=CONTYPE, typename specifies the connection type to trace (such as BATCH, DIST, MASS, SASS).

You can execute CADB2TRC multiple times to active multiple trace types. Each execution produces a list of all active trace requests. A request of TYPE=ALL,TRACE=OFF turns off all tracing requests. All output from CADB2TRC is written to the job log.

Product Releases and Maintenance

New users of CA Top Secret Option for DB2 are provided with a distribution tape containing the current version of the system. Clients are requested to operate only under currently supported releases of CA Top Secret Option for DB2.

Standard user documentation is also provided to CA Top Secret Option for DB2 users. Updates to this documentation are provided automatically to all clients having current maintenance agreements.

Clients with current maintenance agreements also receive ongoing CA Top Secret Option for DB2 maintenance. When a new release of the system is available, a notice is sent to all current CA Top Secret Option for DB2 clients.

Requesting Enhancements

CA Technologies welcomes your suggestions for product enhancements. All suggestions are considered and acknowledged. See the following steps for submitting a suggestion:

1. Logon to CA Technologies support web site at ca.com\supportconnect.
2. Select the Suggestion Box located on the left side of your screen under CONTACT.
3. In the Search By box select Product.
4. Enter eTrust CA-Top Secret Option for DB2 and select Go.
5. Check the box next to eTrust CA-Top Secret Security Option for DB2 - MVS.
6. Select View Submitted Suggestions to view current requested enhancements. If your enhancement has not been suggested, select Add Customer Suggestions.

Index

N

O

P

R

S

T

U

W