Db2 11 for z/OS

Requirements for the Common Criteria



SC19-4011

Notes

Before using this information and the product it supports, be sure to read the general information under "Notices" at the end of this information.

Subsequent editions of this PDF will not be delivered in IBM Publications Center. Always download the latest edition from PDF format manuals for Db2 11 for z/OS (Db2 Home).

2020-06-17 edition

This edition applies to Db2® 11 for z/OS® (product number 5615-DB2), Db2 11 for z/OS Value Unit Edition (product number 5697-P43), and to any subsequent releases until otherwise indicated in new editions. Make sure you are using the correct edition for the level of the product.

Specific changes are indicated by a vertical bar to the left of a change. A vertical bar to the left of a figure caption indicates that the figure has changed. Editorial changes that have no technical significance are not noted.

© Copyright International Business Machines Corporation 2007, 2017.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this information..... v
Who should read this information.....v
Db2 Utilities Suite for z/OS.....v
Terminology and citations.....v
Accessibility features for Db2 11 for z/OS.....vi
How to send your comments..... vi

Chapter 1. Introduction to the Common Criteria..... 1

Chapter 2. Security environment for the evaluated configuration of Db2..... 3
Organizational security policies.....3
Security objectives.....3
IT security objectives..... 3
Non-IT security objectives..... 4
Physical security..... 4
Personnel requirements for the Common Criteria.....4
Procedural requirements for the Common Criteria (Labeled Security only).....5
Connections to Db2.....5
Threats to Db2.....5

Chapter 3. Hardware configuration..... 7
Supported IBM Z hardware..... 7
Supported peripherals..... 7

Chapter 4. Installation requirements for the Common Criteria-evaluated configuration of Db2..... 9
Evaluated configuration software..... 11
z/OS installation.....12
Db2 installation options and restrictions.....12
Disabling the installation SYSADM and installation SYSOPR authorization IDs.....16

Chapter 5. System configuration..... 19
Identification and authentication.....19
RACF password configuration..... 19
RACF configuration..... 20
RACF resource classes..... 20
Limiting concurrent sessions for a user..... 23
Access control.....24
Data sets.....24
Disk and tape volumes..... 26
Devices..... 27
TCP/IP communication..... 27
Mandatory access control (Labeled Security only).....28
RACF configuration for mandatory access control.....28
Mandatory access control in z/OS..... 28
Mandatory access control in Db2..... 29
Discretionary access control..... 30
Discretionary access control in z/OS..... 30
Discretionary access control in Db2..... 30

z/OS users and groups....31
Creation of user profiles....31
Creation of group profiles....31
z/OS user roles....32
Db2 user roles....32
Security-related audits....33
Audit data protection....33
Object reuse....33

Chapter 6. Common Criteria resources....35

Information resources for Db2 11 for z/OS and related products....37

Notices....39
Programming interface information....40
Trademarks....40
Terms and conditions for product documentation....41
Privacy policy considerations....41

Glossary....43

Index....45

About this information

This information describes the Common Criteria-evaluated version of Db2 11 for z/OS.

It provides detailed information about installing and configuring Db2 11 to comply with the Common Criteria. For detailed information about installing and configuring z/OS V1R13, a prerequisite of the evaluated configuration of Db2 11, see z/OS V1R13.0 Planning for Multilevel Security and the Common Criteria.

Throughout this information, "Db2" means "Db2 11 for z/OS". References to other Db2 products use complete names or specific abbreviations.

Who should read this information

This information is intended for those people who are responsible for installing Db2 or managing Db2 security. It is primarily intended for those who plan to install Db2 to be Common Criteria compliant and maintain a Common Criteria-evaluated configuration of Db2.

Db2 Utilities Suite for z/OS

Important: In Db2 11, the Db2 Utilities Suite for z/OS is available as an optional product. You must separately order and purchase a license to such utilities, and discussion of those utility functions in this publication is not intended to otherwise imply that you have a license to them.

Db2 11 utilities can use the DFSORT program regardless of whether you purchased a license for DFSORT on your system. For more information, see the following informational APARs:

- II14047
- II14213
- II13495

Db2 utilities can use IBM® Db2 Sort for z/OS (5655-W42) as an alternative to DFSORT for utility SORT and MERGE functions. Use of Db2 Sort for z/OS requires the purchase of a Db2 Sort for z/OS license. For more information about Db2 Sort for z/OS, see Db2 Sort for z/OS.

Related concepts

Db2 utilities packaging (Db2 Utilities)

Terminology and citations

When referring to a Db2 product other than Db2 for z/OS, this information uses the product's full name to avoid ambiguity.

About the Db2 brand change: IBM has re-branded DB2® to Db2, and Db2 for z/OS is now the name of the offering previously know as "DB2 for z/OS". During and after implementation of this change, you might sometimes still see references to the original names, such as "DB2 for z/OS" and "DB2", in different IBM web pages and documents. However, assume that these refer to the same "Db2 for z/OS" product when the PID, Entitlement Entity, version, modification, and release information match. For more information, see Revised naming for IBM Db2 family products on IBM z/OS platform.

The following terms are used as indicated:

Db2
Represents either the Db2 licensed program or a particular Db2 subsystem.

Tivoli® OMEGAMON® XE for Db2 Performance Expert on z/OS
Refers to any of the following products:

- IBM Tivoli OMEGAMON XE for Db2 Performance Expert on z/OS

© Copyright IBM Corp. 2007, 2017

- IBM Db2 Performance Monitor on z/OS
- IBM Db2 Performance Expert for Multiplatforms and Workgroups
- IBM Db2 Buffer Pool Analyzer for z/OS

C, C++, and C language
Represent the C or C++ programming language.

CICS®
Represents CICS Transaction Server for z/OS.

IMS
Represents the IMS Database Manager or IMS Transaction Manager.

MVS™
Represents the MVS element of the z/OS operating system, which is equivalent to the Base Control Program (BCP) component of the z/OS operating system.

RACF®
Represents the functions that are provided by the RACF component of the z/OS Security Server.

Accessibility features for Db2 11 for z/OS

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in z/OS products, including Db2 11 for z/OS. These features support:

- Keyboard-only operation.
- Interfaces that are commonly used by screen readers and screen magnifiers.
- Customization of display attributes such as color, contrast, and font size

Tip: The IBM Knowledge Center (which includes information for Db2 for z/OS) and its related publications are accessibility-enabled for the IBM Home Page Reader. You can operate all features using the keyboard instead of the mouse.

Keyboard navigation

For information about navigating the Db2 for z/OS ISPF panels using TSO/E or ISPF, refer to the *z/OS TSO/E Primer*, the *z/OS TSO/E User's Guide*, and the *z/OS ISPF User's Guide*. These guides describe how to navigate each interface, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

Related accessibility information

IBM and accessibility

See the *IBM Accessibility Center* at http://www.ibm.com/able for more information about the commitment that IBM has to accessibility.

How to send your comments

Your feedback helps IBM to provide quality information. Please send any comments that you have about this book or other Db2 for z/OS documentation.

Send your comments by email to db2zinfo@us.ibm.com and include the name of the product, the version number of the product, and the number of the book. If you are commenting on specific text, please list the location of the text (for example, a chapter and section title or a help topic title).

Chapter 1. Introduction to the Common Criteria

A *Common Criteria-evaluated subsystem* is a subsystem that has been evaluated according to the Common Criteria, an internationally recognized ISO standard (ISO 15408) that evaluates the security of IT products. You can configure a Db2 subsystem that complies with the Common Criteria.

An environment with the following products contains the technology to meet the requirements of the Common Criteria assurance level EAL4 augmented by ALC_FLR.3 with controlled access and labeled security:

- The Common Criteria Evaluated Base for z/OS Version 1 Release 13 Package
- The Common Criteria Evaluated Base for IBM Resource Access Control Facility (RACF) for z/OS Version 1 Release 13
- The Common Criteria Evaluated Base for Db2 Db2 11 for z/OS Package

See “Evaluated configuration software” on page 11 for more information about the package contents.

The subsystem configuration that meets these Common Criteria requirements is referred to as the *evaluated configuration* in this information. The evaluated configuration allows two modes of operation: Controlled access and labeled security. The labeled security mode is a strict superset of the controlled access mode. Both modes support access controls that are capable of enforcing access limitations on individual users, data, and objects. Both modes provide an audit capability that records security-relevant events that occur within the subsystem.

The same software elements are used in both controlled access and labeled security modes. The two modes have different RACF classes active and require different RACF (SETROPTS) options to be set. All other z/OS configuration parameters are identical in the two modes. Information that pertains only to the controlled access mode is marked as follows: **Controlled Access only**. Information that pertains only to the labeled security mode is marked as follows: **Labeled Security only**.

The controlled access mode provides a single class of access control mechanism: discretionary access control. The labeled security mode provides two classes of access control mechanisms: discretionary and mandatory access controls.

Discretionary access control allows individual users to specify how resources (such as files) under their control can be shared. Discretionary access control restricts access to objects based on the identity of a user, the user's role (if one exists), and the groups to which the user belongs. Discretionary access control ensures that the user is identified as having a “need to know” for the requested resource.

Mandatory access control enforces limitations on sharing of data among users by use of security labels. Mandatory access control is based on the dominance relationships between user security labels and object security labels. One security label dominates another security label when both of the following conditions are true:

- The security level that defines the first security label is greater than or equal to the security level that defines the second security label.
- The set of security categories that defines one security label includes the set of security categories that defines the other security label.

The formal evaluation of Db2 was conducted by an independent licensed laboratory (atsec security information) and certified by a certificate authorizing scheme (Bundesamt für Sicherheit in der Informationstechnik). Conformance claims can be found in the IBM Db2 11 for z/OS Security Target that is posted on the certifier's website (https://www.bsi.bund.de/EN/Home/home_node.html) at the time of certification. The evaluation of Db2 11 for z/OS did not include all Db2 security functions or all methods of achieving the required level of security. You can use security functions that have not been evaluated, or you can use methods of achieving the required level of security that have not been evaluated. However, if you decide to use functions or methods that have not been formally evaluated, you no longer run the evaluated configuration, and you assume responsibility for the security characteristics of the subsystem.

© Copyright IBM Corp. 2007, 2017

This information supersedes other information in the Db2 11 for z/OS library in cases where there is conflicting information. Therefore, use this information if you want to set up a Db2 11 for z/OS subsystem to meet the requirements of the Common Criteria.

Chapter 2. Security environment for the evaluated configuration of Db2

The evaluated configuration is assured to provide effective security measures in a cooperative non-hostile environment only if the configuration is installed, managed, and used correctly.

You must manage the operational environment according to this information.

Organizational security policies

An *organizational security policy* is a set of rules or procedures that is imposed by an organization on its operations to protect its sensitive data.

The organizational security policies that are required by the evaluated configuration are as follows:

- Only those users who have been authorized to access the information within the system can access the system.
- The system must limit the access to viewing of, modification of, and destruction of the information in protected resources to those authorized users who have a “need to know” that particular information.
- The users of the system are held accountable for their actions within the system.
- **Labeled Security only**: The system must limit the access to information based on the following criteria:
  - Sensitivity of the information that is contained in objects, as represented by a label
  - Formal clearance of users to access that information, as represented by user profiles

  Enforcing the access rules prevents a user from accessing information that is of higher sensitivity than the user is operating at and prevents a user from causing information to be downgraded to a lower sensitivity.

  The method for classification of information is made based on criteria that are defined by the organization. This classification is usually based on relative value to the organization and its interest to limit dissemination of that information. The determination of classification of information is outside the scope of the IT system; the IT system is expected only to enforce the classification rules, not to determine classification. The method for determining clearances is also outside the scope of the IT system and is based on the trust that the organization places in individual users and to some extent on the individual's role within the organization.

Security objectives

Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to oppose identified threats and comply with any organizational security policies.

IT security objectives

The *IT security objectives* that you create set goals of security for the system of hardware, software, and firmware of the evaluated configuration. You rely on the IT security objectives to correctly enforce the security policy.

The IT security objectives of the system of hardware, software, and firmware of the evaluated configuration are as follows:

- The system must ensure that only authorized users gain access to the evaluated configuration and its resources.
- The system must control access to resources based on the identity of users. The system must allow authorized users to specify which users can access which resources.

© Copyright IBM Corp. 2007, 2017

- **Labeled Security only**: The system must control access to resources by evaluating the sensitivity of the information that is being accessed and the clearance of the user who is attempting to access that information.
- The system must record the security-relevant actions of users of the evaluated configuration. The system must make this information available to authorized administrators.
- **Labeled Security only**: The system must ensure that any information that is contained in a protected resource is not declassified when the resource is reused.
- The system must provide all of the functions and facilities that are necessary to support the authorized administrators who are responsible for managing the security of the evaluated configuration.
- The system must be designed and implemented in a manner that ensures that the organizational policies are enforced in the evaluated configuration.
- The system must be designed and implemented in a manner that allows for establishing a trusted channel between the evaluated configuration and another trusted IT product, and that protects the user data that is transferred over this channel from disclosure and undetected modification.

Non-IT security objectives

The evaluated configuration is assumed to be complete and self-contained and, as such, is not dependent on any other products to perform properly. However, certain non-IT objectives with respect to the general operating environment must be met.

The non-IT security objectives are as follows:

- Individuals who are responsible for the evaluated configuration must ensure that the evaluated configuration is delivered, installed, managed, and operated in a manner that maintains IT security objectives.
- Individuals who are responsible for the evaluated configuration must ensure that the parts of the evaluated configuration that are critical to security policy are protected from physical attacks that might compromise IT security objectives.
- Individuals who are responsible for the evaluated configuration must ensure that all access credentials, such as passwords or other authentication information, are protected by the users in a manner that maintains IT security objectives.
- The underlying hardware must provide a separation mechanism that can be used by the evaluated configuration to protect the evaluated configuration and the data that it contains from unauthorized access and modification.
- **Labeled Security only:** Individuals who are responsible for the evaluated configuration must ensure that users of the evaluated configuration are cleared for access to information. Individuals who are responsible for the evaluated configuration must evaluate the classification of the information and ensure that information is correctly classified for protection by the security functions of the evaluated configuration.

Physical security

For a Db2 Common Criteria system to be considered secure, the hardware and firmware components that provide the physical environment for the evaluated configuration are required to be physically protected from unauthorized access and physical modification. Also, Db2 must be running in a z/OS Common Criteria controlled environment.

Personnel requirements for the Common Criteria

One or more qualified individuals must be assigned to manage the evaluated configuration and the security of the information that it contains. These authorized users must act in a cooperating manner and follow the instructions in this information and other guidance information.

Assign all individual users a unique user ID and specific security label, and grant users access to objects based on existing procedures.

Labeled Security only: Every individual must be associated with a security label.

Procedural requirements for the Common Criteria (Labeled Security only)

The ability of the evaluated configuration to enforce the intent of the organizational security policy, especially with regard to the mandatory access controls, is dependent on the establishment of procedures.

Create the following procedures to protect the data:

- Permit users authorization to specific security labels
- Establish the security label of all important information
- Mark a security label on all generated output
- Establish the security label of all peripheral devices (such as printers, disk drives, tape drives)

Connections to Db2

Only IBM Z to IBM Z connections are allowed in the evaluated configuration. Any other systems that the evaluated configuration communicates with must be under the same management control and operate under the same security constraints as the evaluated configuration.

Certificate-based connections to the evaluated configuration are not allowed. Do not create a distributed identity filter to map a Db2 authorization ID associated with a certificate to a RACF user ID. In other words, do not define a mapping association between a RACF user ID and an authorization ID that is both authorized to access Db2 and associated with a certificate.

All connections to other systems must reside within the controlled access facilities unless they are protected by the Secure Socket Layer (SSL) or IPSec protocol. Db2 supports the SSL protocol by using the z/OS Communications Server IP Application Transparent Transport Layer Security (AT-TLS). Internal communication paths to access points such as terminals or job entry stations, and communication links that use Distributed Relational Database Architecture™ (DRDA) to access Db2, are assumed to be adequately protected by measures in the evaluated configuration environment.

When you set up connections for labeled security, the content of the security label of the user varies depending on the connection that is used with Db2:

- For local connections, the security label of the user is the label that the user used during sign-on.
- For TCP/IP connections, the security label of the user is defined by the security zone.
- For trusted connections, the security label can be associated with the user based on the trusted context definition.

Related concepts

Encrypting your data with Secure Socket Layer support (Managing Security)

Security labels (Managing Security)

Related reference

RACF RACMAP command (create, delete, list, or query a distributed identity filter) (Security Server RACF Command Language Reference)

Threats to Db2

Threats to the evaluated configuration are violations of the organizational security policies that are defined in this information.

The IT assets that are to be protected comprise the data that is stored, processed, or transmitted by the evaluated configuration. The term *data* is used here to refer to all data that is held within the evaluated configuration, including data that is in transit between different systems as part of a Parallel Sysplex® environment.

The threat agents can be categorized as one of the following types of users:

- Unauthorized users of the evaluated configuration, such as individuals who have not been permitted the right to access the system

- Authorized users of the evaluated configuration, such as individuals who have been permitted the right to access the system

The threat agents are assumed to originate from a well-managed user community in a working environment, and the evaluated configuration therefore protects against threats of inadvertent or casual attempts to breach the system security. The evaluated configuration is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile attackers with a high level of expertise to breach system security.

Chapter 3. Hardware configuration

For the evaluated configuration to remain Common Criteria-compliant, it must operate on a secure hardware configuration.

Supported IBM Z hardware

Db2 11 for z/OS operates on z10 or later processors running z/OS V1.13, or later.

The acceptable hardware platforms are as follows:

- IBM System z10® Enterprise Class (z10 EC) or later
- IBM System z10 Business Class (z10 BC) or later

Supported peripherals

You must place the peripheral devices and their connections within the controlled access facilities unless they are protected by the Secure Socket Layer (SSL) or IPSec protocol. Db2 supports the SSL protocol by using the z/OS Communications Server IP Application Transparent Transport Layer Security (AT-TLS).

Prior to installation, you must develop procedures for establishing physical security for all peripheral devices (such as printers, disk drives, and tape drives) that are attached to the evaluated configuration.

You can use the following peripherals with the evaluated configuration:

- Terminals
- Printers
  - **Controlled Access only:** any printer that is supported by the evaluated configuration.
  - **Labeled Security only:** any printer that is used to print output with different security labels must support the Guaranteed Print Labeling function. Guaranteed print labeling works with a subset of Advanced Function Presentation (AFP) printers and ensures the integrity of the identification label by preventing the user from changing the label. Review the printer hardware documentation or contact the printer vendor to determine if a printer supports this function.
- Storage devices and backup devices such as disk and tape drives
- Ethernet and token-ring network adapters

You can connect to peripherals within the evaluated configuration environment if the evaluated configuration executes within a logical partition (LPAR). Virtual devices are allowed in an LPAR environment because the logical partitioning software is part of the hardware, and therefore part of the evaluated configuration environment.

Related concepts

Encrypting your data with Secure Socket Layer support (Managing Security)

© Copyright IBM Corp. 2007, 2017

Chapter 4. Installation requirements for the Common Criteria-evaluated configuration of Db2

You must satisfy all the requirements for installing the Common Criteria-evaluated configuration of Db2.

Installation of the evaluated configuration of Db2 consists of the following steps:

1. Read this document in its entirety.
2. Verify the integrity of the package that you received: the cardboard box must be wrapped with glass tape with all seams covered and there must be no sign of rewrapping or attempt to open the box. Tapes that are included in the box must be shrink-wrapped as well.
3. Verify that the labels of the ServerPacs that were shipped correspond to the packages that are enumerated in the “Evaluated configuration software” on page 11 section of this document. Additional PTFs might be listed in the memo that is enclosed in the package.
4. Install the ServerPac according to the Installing Your Order document that accompanies the ServerPac, taking into account the exceptions that are described in the following topics.
5. Install the unintegrated service that is shipped with the ServerPac that applies to your subsystem.
6. Install the service that is delivered on the media that accompanies the ServerPac.
7. Install the remaining unintegrated service that is shipped with the ServerPac and that did not apply in step 3.
8. Configure your new subsystem with the options that are described in the following topics.

Before you install the evaluated configuration of Db2, become familiar with the normal Db2 installation process. For overview information about a standard installation of Db2, see Installing and migrating Db2 (Db2 Installation and Migration).

The evaluated configuration of Db2 must be installed with a ServerPac installation using the "Full System Replace" installation option. Failure to do so results in a non-evaluated configuration.

Follow the instructions in the ServerPac: Installing Your Order document with the following exceptions:

- During Db2 installation CLIST processing, on Distributed data facility panel 2: DSNTIP5, ensure that the TCP/IP ALREADY VERIFIED field is set to the default value of NO. A value of NO results in a DSNZPARM value TCPALVER=NO in job DSNTIJUZ and is required for the evaluation configuration.
- Job DSNTIJEX: Db2 sample authorization exits

  Use of the Db2 RACF authorization exit routine (DSNXRXAC) is required and built by Db2 installation job DSNTIJEX. However, the use of other sample authorization exits that are built in DSNTIJEX are restricted by the evaluated configuration and must be removed. To remove these other sample authorization exits, modify the job as follows:

  – Delete step JEX0001. JEX0001 assembles the Db2 sign-on exit, DSN3SSGN/DSN3@SGN, the use of which is restricted.
  – Delete step JEX0002. JEX0002 assembles the Db2 identify exit, DSN3SATH/DSN3@ATH. the use of which is restricted.
  – Modify step JEX0003 to refer to DSNX**R**XAC(MEM=DSNX**R**XAC) instead of DSNX**S**XAC. DSNXRXAC is the required RACF external security module that is used as the Db2 access control authorization exit.
  – Delete step JEX0004. JEX0004 assembles the user exit for the DSNACICS stored procedure, DSNASCIX/DSNACICX, the use of which is restricted.
- Installing Your Order, section 5.2: IPLing z/OS and Starting Your New Db2 System.

  Job DSNTIJTC requires installation SYSADM instead of SYSADM.
- Installing Your Order, section 5.3: Logging on to TSO/E

© Copyright IBM Corp. 2007, 2017

Define the Db2 SYSADM authorization ID to RACF or UADS with ALTER authority for all system resources, such as catalogs. Enter the authorization ID that has Db2 SYSADM authority for the SYSADM parameter.

To enable primary authorization IDs to issue Db2 commands from the z/OS console or TSO SDSF, use the following statements to define RACF classes that authorize Db2 commands:

```
SETR CLASSACT(DSNADM)
RDEFINE DSNADM DSN1.SYSOPR UACC(NONE)
PERMIT DSN1.SYSOPR CLASS(DSNADM) ID(userid) ACCESS(READ)
SETR RACLIST(DSNADM) REFRESH
```

- Job DSNTIJSG: Define and bind Db2 objects and user-maintained databases

  Do not use the Db2 GRANT SQL statements that are provided in this job. The evaluated configuration requires that you use the RACF external security module, DSNXRXAC, that is defined in installation job DSNTIJEX, instead of Db2 GRANT or REVOKE SQL statements. Modify DSNTIJSG and delete or comment out job step DSNTIJG entirely.

  Do not use Java™ Archives (JAR) objects that would be bound by this job. Modify step DSNTIRU to comment out or delete all BIND commands for PACKAGE(DSNJAR).

  In the Labeled Security mode, restrictions apply to some Db2 functions because the required Db2 objects that are created in DSNTIJSG do not have Labeled Security-required security labels defined and the CREATE SQL statements fail. Modify job steps DSNTIRL, DSNTIJR, DSNTIJQ, and DSNTIJP to comment out or delete all the objects and any dependant indexes.

- Job DSNTIJRT: Install and configure Db2-supplied routines

  Use the following process to remove GRANT statements and to avoid creating objects that are not supported in the evaluated configuration:

  1. In job step DSNTRIN, change the MODE setting to INSTALL-PREVIEW to generate another job that contains generated DDL and BIND statements for installing Db2-supplied routines. Verify that the JCLOUT DD allocates a partitioned data set and member to receive this job.
  2. Run job DSNTIJRT that should end with a return code of 0 or 4.
  3. Edit the job that was written to the data set and member allocated by the JCLOUT DD. Follow the directions in the job prolog to customize it for your Db2. In addition, make the following additional modifications:

     a. Job step GRNTSTEP: Delete this job step entirely to remove all GRANT statements.

     b. Job step INSTSTEP: Locate and remove all but the following SQL and BIND statements:

```
- BIND PACKAGE(DSNAHVPM) MEMBER(DSNAHVPM) ...
- BIND PACKAGE(DSNACCOR) MEMBER(DSNACCOR) ...
- BIND PACKAGE(DSNACCOX) MEMBER(DSNACCOX) ...
- BIND PACKAGE(DSNTWR) MEMBER(DSNTWR) ...
- BIND PACKAGE(DSNWSPM) MEMBER(DSNWSPM) ...
- BIND PACKAGE(DSNUTILS) MEMBER(DSNUTILS) ...
- BIND PACKAGE(DSNUTILU) MEMBER(DSNUTILU) ...

- CREATE PROCEDURE SYSPROC.DSNAHVPM ...
- CREATE PROCEDURE SYSPROC.DSNACCOR ...
- CREATE PROCEDURE SYSPROC.DSNACCOX ...
- CREATE GLOBAL TEMPORARY TABLE SYSIBM.SYSPSMOUT ...
- CREATE PROCEDURE SYSPROC.DSNTPSMP ...
- CREATE PROCEDURE SYSPROC.WLM_REFRESH ...
- CREATE PROCEDURE SYSPROC.DSNWSPM ...
- CREATE PROCEDURE SYSPROC.DSNWZP ...
- CREATE GLOBAL TEMPORARY TABLE SYSIBM.SYSPRINT ...
- CREATE PROCEDURE SYSPROC.DSNUTILS ...
- CREATE PROCEDURE SYSPROC.DSNUTILU ...
```

     c. Run the job to create and bind the Db2-supplied routines.

- Job DSNTIJIC: Back up the Db2 directory and catalog

If Db2 is started under ACCESS(MAINT), the user on the job statement must be the same user that you specified for either the SYSTEM ADMIN 1 option or the SYSTEM ADMIN 2 option on installation panel DSNTIPP1.

- **Labeled Security only:** Installing Your Order, section 6: Verifying Installation

  It is not recommended that you execute the Db2 installation verification (IVP) jobs in Labeled Security mode because the IVP jobs always fail in Labeled Security mode systems. This is because in Labeled Security mode systems, the Db2 objects that are created by the IVP jobs do not have Labeled Security-required security labels defined on them, so the CREATE SQL statements fail. This does not mean that installation of the evaluated configuration failed.

Related concepts

Db2 installation options and restrictions
The evaluated configuration has strict requirements about which options and elements must be used, which options can be used, and which options cannot be used. Restrictions also apply to how some options and elements can be used.

Introduction to the RACF access control module (RACF Access Control Module Guide)

Evaluated configuration software

The evaluated configuration has strict requirements about which software must be installed, which options can be installed, which external software can be installed, and which options cannot be installed.

The evaluated configuration requires installation of the following packages in the following order:

1. The Common Criteria Evaluated Base for z/OS V1R13 Package, which includes the following software elements:
   - z/OS V1R13 English Base (5694-A01 V1.13.0):
     - ENABLED priced optional features:
       - DFSMS dss
       - RMF
       - SDSF
       - Security Server (RACF)
     - Unpriced features (export-controlled):
       - Communications Server Security Level 3
       - z/OS Security Level 3
     - GI10-0670-13 z/OS V1R13 Program Directory
     - SK3T-4271-29 z/OS V1R13 DVD Collection
     - GA22-7501-21 z/OS Hot Topics Newsletter
     - ServerPac: IYO (Installing Your Order)
     - Memo about z/OS V1R13 Common Criteria Evaluated Base
     - GA22-7509-13 z/OS V1R13.0 Planning for Multilevel Security and the Common Criteria
   - OGL/370 (5688-191 V1.1.0):
     - G544-3691-00 OGL/370 V1.1.0 Getting Started
     - G544-3697-00 OGL/370 V1.1.0 LPS
     - S544-3703-01 OGL/370 Command Summary and Quick Reference
     - GI10-0212-01 OGL/370 Program Directory
   - PSF V4 Base z/OS (5655-M32 V4.4.0):
     a. GI11-9472-00 PSF V4.4 Base Program Directory
     b. SK5T-8814-00 PSF V4.4 Base Library Collection

- IBM Ported Tools for z/OS (5655-M23 V1.2.0):
  - GI10-0769-06 IBM Ported Tools for z/OS V1.2.0 Program Directory
  - GA22-7986-08 IBM Ported Tools for z/OS V1.2.0 License Information

2. The Common Criteria Evaluated Base for Db2 11 for z/OSPackage, which includes the following software elements:
   - Either the standard Db2 11 for z/OS (program number 5635-Db2) or the Db2 11 for z/OS (Value Unit Edition) (program number 5697-P12). This includes the RACF Access Control Module (DSNXRXAC member of *prefix*.SDSNSAMP).
   - Db2 Utilities Suite for z/OS Version 11 (program number 5655-N97).
   - Additional critical PTFs.

Any fixes that are delivered with the two packages must be installed as described in the memos that are delivered with the packages.

z/OS installation

To have an evaluated configuration of Db2, you must use the Common Criteria Evaluated Base for z/OS V1R13 Package.

For detailed information about installing and configuring the Common Criteria-evaluated configuration of z/OS, see z/OS multilevel security and the Common Criteria (Planning for Multilevel Security and the Common Criteria).

Db2 installation options and restrictions

The evaluated configuration has strict requirements about which options and elements must be used, which options can be used, and which options cannot be used. Restrictions also apply to how some options and elements can be used.

The following options and elements must be installed in the evaluated configuration:

- Audit traces
- Installation SYSADM and installation SYSOPR authorization IDs for the initial setup and configuration of Db2

  You must disable the installation SYSADM and installation SYSOPR authorization IDs after installation. For instructions for disabling the installation SYSADM and SYSOPR authorization IDs after installation, see “Disabling the installation SYSADM and installation SYSOPR authorization IDs” on page 16.
- RACF authorization exit routine (DSNXRXAC)

  DSNXRXAC is shipped in *prefix*.SDSNSAMP. Do not customize DSNXRXAC. Use installation job DSNTIJEX to install DSNXRXAC, as explained in Managing security with the RACF access control module. Run only step 3 (JEX0003) in DSNTIJEX and set the error option &ERR0R0PT to 2.
- Subsystem security that is provided by the z/OS Common Criteria environment
- TCP/IP security that is provided by the z/OS Common Criteria environment, if you use distributed data

You can use the following options and elements without changing the security characteristics of the evaluated configuration:

- Call attachment facility
- TSO attachment facility
- RRSAF attachment facility
- IBM utilities

You cannot use the following objects, options, and elements in the evaluated configuration because either they violate the security policies on which the evaluation was based, or they were not evaluated (due to complexity, scheduling, or other reasons). The following objects, options, and elements must not be configured for use, or must be deactivated:

- Administrative task scheduler

  You can disable the administrative task scheduler by issuing one of the following commands from the z/OS console, where *admtproc* is the procedure name of the administrative task scheduler task that is to be stopped:

  MODIFY *admtproc*, APPL=SHUTDOWN
  The MODIFY command waits until all executed tasks finish and then brings down the scheduler, and no new tasks are started.

  STOP *admtproc*
  The STOP command stops the administrative task scheduler and interrupts every task that is currently being executed by the scheduler, so that these tasks get an error status.

  You can also set DSN6SPRM.ADMTPROC in job DSNTIJUZ to blank so that the administrative task scheduler does not attempt to start. When you run the installation CLIST, you can set DSN6SPRM.ADMTPROC in the ADMIN SCHEDULER field on panel DSNTIPX.
- Administrative stored procedures

  Do not use administrative stored procedures.
- CICS connections

  You can disable Db2 processing of CICS transactions in any of the following ways:

  – Define the DSNR class profile subsystem.SASS with ACCESS(NONE).
  – BIND the application (plan or package) with the DISABLE option for connection type CICS.
  – Deactivate from within CICS:

    CICS transaction code security works with RACF to control the transactions and programs that can access Db2. Within Db2, you can use the ENABLE and DISABLE options of the bind operation to limit access to specific CICS subsystems.
- Data propagation products

  Do not install.
- Accelerator Servers

  Do not install.
- Db2 Web Services

  Do not install the Db2 Web Services as described in Enabling Db2 web services (Db2 Installation and Migration). Db2 Web Services depend on JDBC.
- Db2 REST API connections.
- Encryption and decryption built-in functions

  Do not use the encryption or decryption built-in functions.
- GRANT/REVOKE functions

  The GRANT/REVOKE functions will not be used for authorization if RACF profiles are defined for all Db2 objects for which authorization is checked. Defining these RACF profiles ensures that the RACF access control module returns only authorized and not authorized responses, which prevents Db2 grants from being considered in the authorization decision.

  The RACF access control module has error option &ERR0R0PT set to 2, which shuts down Db2 when the RACF module abends or returns an unexpected return code. This setting ensures that authorization is not switched to Db2 if the RACF module malfunctions.
- IMS connections (FMID HIYBB10)

  You can disable Db2 processing of IMS transactions in any of the following ways:

  – Define the DSNR class profile subsystem.MASS with ACCESS(NONE).
  – BIND the application (plan or package) with the DISABLE option for connection type IMS, IMSBMP, IMSMPP and DLIBATCH.

  - Deactivate from within IMS:

    IMS terminal security lets you limit the entry of a transaction code to a particular logical terminal (LTERM) or group of LTERMs in the system. To protect a particular program, you can authorize a transaction code that is to be entered only from any terminal on a list of LTERMs. Alternatively, you can associate each LTERM with a list of the transaction codes that a user can enter from that LTERM. IMS then passes the validated LTERM name to Db2 as the initial primary authorization ID.

- JDBC/SQLJ (FMID JDBBB12)
  - **Db2 Db2 JDBC/SQLJ:** Do not execute Java installation job "db2jdbcbind", which would bind the driver to Db2.
- Java Archives (JAR)

  Before executing installation job is DSNTIJSG, delete all BIND commends for PACKAGE(DSNJAR).
- Kerberos

  Do not enable the use of Kerberos as described in Making the program operational.
- ODBC/CLI (FMID JDBBB17)

  Do not execute installation job DSNTIJCL, which would bind the ODBC driver to Db2.
- PassTickets

  Do not enable the use of PassTickets as described in Enabling the use of PassTickets.
- Secondary authorization IDs

  Do not install DSN3@ATH using the sample connection exit routine that is provided (DSN3SATH). The default connection exit routine from SDSNLOAD is DSN3@ATH and is active if you do not assemble and install DSN3SATH. The default connection exit routine excludes secondary authorization IDs. To use the default, delete step JEX0002, which assembles DSN3@ATH, from installation job DSNTIJEX.
- Sign-on authorization IDs

  Do not install DSN3@SGN using the sample sign-on exit routine that is provided (DSN3SSGN). The default sign-on exit routine from prefix.SDSNLOAD is DSN3@SGN and is active if you do not assemble and install DSN3SSGN. The default sign-on exit routine excludes code-altering authorization IDs at sign-on. To use the default, delete step JEX0001, which assembles DSN3@SGN, from installation job DSNTIJEX.
- SNA connections

  To disable SNA connections, remove all rows from the SYSIBM.LUNAMES table.
- Unified debugger

  Remove the SDSNLOAD(DSNASPDB) and its 15 related aliases:
  - DSNACRSS
  - DSNADTSS
  - DANAEMNG
  - DSNAGTLV
  - DSNAGTRP
  - DSNAINCL
  - DSNALSMG
  - DSNALTSS
  - DSNAPMNG
  - DSNAPTCM
  - DSNAQRSS
  - DSNARCCL
  - DSNASDCM

  - DSNASDRQ
  - DSNATRCL

  Also, remove the SDSNLOAD(DSNAPSMD) Db2 load module.
- User exit routines

  Do not use table-defined edit routines or table-defined field procedures in the evaluated configuration.

  Exception: You must install the RACF authorization exit routine (DSNXRXAC).
- WebSphere® MQ user-defined functions

  Do not install the WebSphere MQ user-defined functions as described in Additional steps for enabling WebSphere MQ user-defined functions (Db2 Installation and Migration).
- z/OSMF installation

  Do not use z/OSMF for Db2 installation.
- z/OS ODBC interface to SQL

  Do not perform the bind packages and plans steps as documented in Configuring Db2 ODBC and running sample applications (Db2 Programming for ODBC).

Restrictions: The following restrictions apply to database objects and user security:

- Protection panel: DSNTIPP

  When you install Db2, you cannot accept the default values for the following security-related fields on panel DSNTIPP:

  - PACKAGE AUTH CACHE, subsystem parameter CACHEPAC

    The default value of PACKAGE AUTH CACHE is non-zero, but must be set to zero because package authorization caching is excluded from the evaluated configuration.
  - ROUTINE AUTH CACHE, subsystem parameter CACHERAC

    The default value of ROUTINE AUTH CACHE is non-zero, but must be set to zero because routine authorization caching is excluded from the evaluated configuration.
  - AUTH EXIT CHECK, subsystem parameter AUTHEXIT_CHECK

    The default value of AUTHEXIT_CHECK is PRIMARY, but must be set to DB2 because the object owner is used for authorization checks, where applicable, in the evaluated configuration.
- Distributed data facility panel 1: DSNTIPR

  When you install Db2, you cannot accept the default value for the following security-related field on panel DSNTIPR:

  - EXTENDED SECURITY, subsystem parameter EXTSEC

    The default value of EXTENDED SECURITY is YES, but must be set to NO to prevent RACF users from changing their passwords and because descriptive security error codes are excluded from the evaluated configuration.
- **Labeled Security only:** You must set the COMCRIT parameter to YES in a Common Criteria Labeled Security environment. The effect of changing the value of the COMCRIT parameter to YES is that every table that is created must have multilevel security. The parameter is set by changing the value of COMCRIT from the default of NO to YES in job DSNTIJUZ during installation. Setting the COMCRIT parameter to YES causes the optional installation IVP jobs to produce error messages that do not affect the success of the installation. See COMCRIT in macro DSN6SPRM (Db2 Installation and Migration).

  Labeled Security only: The following functions do not operate in Labeled Security mode because they use tables that do not have a security label column:

  - EXPLAIN
  - REORG TABLESPACE using the SHRLEVEL CHANGE
  - Resource Limit Facility (RLF)

When Db2 is started in a Labeled Security Common Criteria environment, Db2 issues SQLCODE -4738 under the following circumstances:

- Whenever a CREATE TABLE statement does not include a column with the AS SECURITY LABEL clause. Every normal base table must include a security label column in a Labeled Security Common Criteria environment.
- Whenever a CREATE or ALTER TABLE statement attempts to define a materialized query table. You cannot define materialized query tables in a Labeled Security Common Criteria environment.
- Whenever the LIKE or AS (fullselect) clauses are specified as part of a CREATE TABLE or DECLARE GLOBAL TEMPORARY TABLE statement. These clauses are not supported in a Labeled Security Common Criteria environment.

Controlled Access only: You must set the COMCRIT parameter to NO in a Common Criteria Controlled Access environment. If the value of COMCRIT is NO, tables cannot be created with a column defined with the AS SECURITY LABEL clause.

- You can create user-maintained databases only when Db2 objects are protected by RACF.
- System data sets must be RACF-controlled. These include underlying data sets for user data and indexes, archive logs, active logs, bootstrap data sets (BSDSs), online library, work file data sets, sort file data sets, catalog and directory data sets, and data sets that are used to collect statistics or EXPLAIN history.
- **Labeled Security only:** To run certain LOAD, UNLOAD, and REORG TABLESPACE utility jobs, you need a valid security label and additional authorizations.

Related concepts

Installation requirements for the Common Criteria-evaluated configuration of Db2
You must satisfy all the requirements for installing the Common Criteria-evaluated configuration of Db2.

Db2 utilities (Db2 Utilities)

Related tasks

Installing and migrating Db2 (Db2 Installation and Migration)

Disabling the installation SYSADM and installation SYSOPR authorization IDs

After installing Db2, you can disable the installation SYSADM and installation SYSOPR authorization IDs.

About this task

The DSNTIPP1: Protection panel 2 (Db2 Installation and Migration) defines the values of the installation SYSADM and installation SYSOPR authorization IDs in the following fields:

- SYSTEM ADMIN 1
- SYSTEM ADMIN 2
- SYSTEM OPERATOR 1
- SYSTEM OPERATOR 2

The values of the installation SYSADM and installation SYSOPR authorization IDs require a valid RACF authorization ID for proper installation.

The values that are defined in the fields on DSNTIPP1: Protection panel 2 (Db2 Installation and Migration) result in the following fields in the Db2 Parameter Module:

- &SYSADM
- &SYSADM2
- &SYSOPR1
- &SYSOPR2

The Db2 Parameter Module is defined during installation on the DSNTIPO3: Default startup modules panel (Db2 Installation and Migration). The default file name is DSNZPARM.

However, to have a Common Criteria compliant Db2 subsystem, all authorization IDs must use the external authorization software product Resource Access Control Facility (RACF). In Db2, if the authorization ID that is being verified is the installation SYSADM or installation SYSOPR authorization ID, RACF is not invoked and all Db2 privileges of SYSADM or SYSOPR are permitted.

Therefore, to meet the requirements for Common Criteria compliance, the installation SYSADM and installation SYSOPR authorization IDs must be disabled after Db2 installation is completed.



CAUTION: Installation SYSADM and installation SYSOPR privileges can be required for critical events and are required to run the SYSTEM RESTORE Db2 utility. Have well-defined procedures in place to enable the installation SYSADM and installation SYSOPR authorization ID privileges.

Example

Assume you define the following RACF ID to be Db2 installation SYSADM with the privileges that are usually associated with a RACF ID SYSADM1:

```
ADDUSER SYSADM1 SECLABEL(SYSHIGH) PASSWORD(password)
ALTUSER SYSADM1 PASSWORD(password) NOEXPIRED
PERMIT SYSHIGH  CLASS(SECLABEL) ACCESS(ALTER) ID(SYSADM1)
PERMIT DB2A.SYSADM ID(SYSADM1) ACC(UPDATE) CL(DSNADM)
PERMIT DB2A.BATCH  ID(SYSADM1) ACC(UPDATE) CL(DSNR)
```

where *password* is your subsystem password

1. To disable the RACF ID that is defined as the Db2 installation SYSADM authorization ID, issue the following command:

   ```
   ALTUSER  SYSADM1 REVOKE
   ```

   The REVOKE option specifies that RACF is to prevent the user from accessing the system. The user's profile and data set profiles are not deleted from the RACF database.
2. Also force this user from THE SYSTEM, for example the user may already be logged on TSO.

   ```
   C U=SYSADM1
   ```

What to do next

To re-enable the RACF ID that is defined as the Db2 installation SYSADM authorization ID, issue the following command:

```
ALTUSER  SYSADM1 RESUME
```

The RESUME option specifies that the user can access the system again and is typically used to restore a user's access to the system that has been prevented by a prior REVOKE command.

Related reference

RACF commands (Security Server RACF Command Language Reference)

Chapter 5. System configuration

You use both mandatory and optional parameters and controls to configure your evaluated configuration.

You must configure the mandatory requirements as stated to maintain the minimum level of security that the evaluated configuration requires. You can choose which options to implement based on a security policy that matches your own security requirements.

Identification and authentication

Users are identified and authenticated by a user ID and password combination before being authorized to perform any other security-relevant action.

Users can choose their own passwords, their default group, and their user IDs.

Labeled Security only: Users can choose their security levels when they log in.

A user can interact with the evaluated configuration in one of the following ways:

- As a TSO user
- As a UNIX user
- As a user connecting to the DRDA interface of Db2
- As an operator at a console
- Through the association with a trusted context that is established by an external entity
- By submitting a job that is to be initiated and scheduled by the Job Entry Subsystem (JES2)

In the case of jobs that are submitted by a user who is already authenticated, no additional authentication is required for jobs that run with the ID of the user who submitted them. The internal reader accepts (and relies) in this case on the authentication that was performed when the user logged on to TSO.

Exception: Started tasks with the TRUSTED or PRIVILEGED attribute operate under a protected user ID and are started either at system startup or through an operator command. These tasks do not execute on behalf of a human user, and their protected user IDs cause all authentication checks to pass. They must be started only from trusted data sets.

RACF password configuration

To remain Common Criteria-compliant, you must enforce certain rules for RACF passwords.

Users must select their own passwords, and only they can know their passwords. If a password needs to be reset, the security administrator must reset the password. This new password must be in an expired state, which forces the user to enter a new password on the first logon.

Exception: When a new user ID for a pseudo-user is created and the pseudo-user is not a protected user ID, the initial password can be marked as unexpired.

Determine the rules for forming valid passwords. To make the rules system-wide, use the SETROPTS command. To make the rules specific to a single user, use the PASSWORD command. For more information about the rules for RACF passwords, see z/OS multilevel security and the Common Criteria (Planning for Multilevel Security and the Common Criteria).

Related concepts

Introduction to the RACF access control module (RACF Access Control Module Guide)

Related reference

z/OS multilevel security and the Common Criteria (Planning for Multilevel Security and the Common Criteria)

© Copyright IBM Corp. 2007, 2017

RACF configuration

You must configure RACF with certain options.

To conform with the evaluated configuration, configure RACF with the following options (using the RACF SETROPTS command):

- CATDSNS(FAILURES)
- CLASSACT(TEMPDSN)
- ERASE(ALL)
- GENERIC(*)
- GRPLIST
- JES(BATCHALLRACF)
- NOCOMPATMODE
- PASSWORD
- PROTECTALL(FAILURES)
- **Labeled Security only:** MLACTIVE(FAILURES)
- **Labeled Security only:** MLFSOBJ(ACTIVE)
- **Labeled Security only:** MLIPCOBJ(ACTIVE)
- **Labeled Security only:** MLS(FAILURES)
- **Labeled Security only:** MLSTABLE
- **Labeled Security only:** SECLABELAUDIT
- **Labeled Security only:** SECLABELCONTROL

All other RACF options are optional.

Related concepts

Introduction to the RACF access control module (RACF Access Control Module Guide)

Related reference

RACF commands (Security Server RACF Command Language Reference)

RACF security administration (Security Server RACF Security Administrator's Guide)

RACF resource classes

You can use RACF resource classes to protect system objects.

The evaluated configuration covers the protection that is provided by the Db2-related RACF resource classes that are shown in the following table.

Table 1. Db2-related RACF resource classes

Class	Function
DSNADM	Controls Db2 administrative authority.
DSNR	Controls access to Db2 subsystems.
GDSNBP or MDSNBP	Controls access to Db2 buffer pools.
GDSNCL or MDSNCL	Controls access to Db2 collections.
GDSNDB or MDSNDB	Controls access to Db2 databases.
GDSNGV or MDSNGV	Controls access to Db2 global variables.

Table 1. Db2-related RACF resource classes (continued)

Class	Function
GDSNJR or MDSNJR	Controls access to Db2 Java archive files. **Restriction:** You cannot access Java archive files in the evaluated configuration.
GDSNPK or MDSNPK	Controls access to Db2 packages.
GDSNPN or MDSNPN	Controls access to Db2 plans.
GDSNSC or MDSNSC	Controls access to Db2 schemas.
GDSNSG or MDSNSG	Controls access to Db2 storage groups.
GDSNSM or MDSNSM	Controls Db2 privileges.
GDSNSP or MDSNSP	Controls access to Db2 stored procedures.
GDSNSQ or MDSNSQ	Controls access to Db2 sequences.
GDSNTB or MDSNTB	Controls access to Db2 tables, indexes, and views.
GDSNTS or MDSNTS	Controls access to Db2 table spaces.
GDSNUF or MDSNUF	Controls access to Db2 user-defined functions.[1]
GDSNUT or MDSNUT	Controls access to Db2 user-defined types.[1]

Note: You can use user-defined types and user-defined functions, but they are not part of the evaluated configuration. RACF resource classes GDSNUF, MDSNUF, GDSNUT, and MDSNUT do not protect or otherwise influence the other classes that are defined for Db2 objects.

The evaluated configuration also covers the protection that is provided by the generic RACF resource classes that are shown in the following table.

Table 2. Generic RACF resource classes

Class	Function
CONSOLE	Controls access to MCS or SMCS consoles. Also controls conditional access to other resources for commands that originate from an operator console.
DASDVOL	Controls access to DASD volumes for maintenance operations.
DEVICES	Controls access to unit record devices, teleprocessing or communication devices, and graphic devices.
DIRAUTH[1]	Ensures that security label authorization checking is done when a user receives a message that is sent through the TPUT macro or the TSO SEND or LISTBC commands. Profiles are not allowed in this class.
FACILITY	Used by various components of the evaluated configuration to manage specific privileges that can be assigned to users so that they do not need the SPECIAL attribute.
GLOBAL	Defines the entries in the global access checking table.

Table 2. Generic RACF resource classes (continued)

Class	Function
GTERMINL	Resource group class for TERMINAL class.
JESINPUT	Port of entry class to control which JES2 input devices a user can use to submit batch work to the system.
JESJOBS	Controls the submission and cancellation of jobs by job name.
JESSPOOL	Controls access to job data sets on the JES spool (that is, SYSIN and SYSOUT data sets).
NODES	Controls the following factors on z/OS systems: • Whether jobs are allowed to enter the system from other JES2 nodes. • Whether jobs that enter the system from other nodes must pass user identification and password verification checks.
OPERCMDS	Controls who can issue operator commands.
PROGRAM	Controls access to programs (load modules).
PSFMPL	Used by Print Services Facility (PSF) to perform security functions for printing, such as separator page labeling, data page labeling, and enforcement of the user printable area.
SDSF	Controls the use of authorized commands in the System Display and Search Facility (SDSF).
Labeled Security only: SECDATA	Controls security classification of users and data (security levels and security categories).
Labeled Security only: SECLABEL	Controls security labels.
SERVAUTH	Controls a client's authorization to use a server or to use resources that are managed by the server.
SERVER	Controls the validity of servers for the application environment.
SMESSAGE	Controls to which users a user can send messages (TSO only).
STARTED	Assigns an identity to a started task during the processing of a z/OS START command. Use STARTED as an alternative to the started procedures table (ICHRIN03).
TAPEVOL	Controls access to tape volumes.
TERMINAL	Controls access to terminals (TSO/E).
TSOPROC	TSO logon procedures.
UNIXPRIV	Used to grant z/OS UNIX privileges.
VTAMAPPL	Controls who can open ACBs from non-APF-authorized programs. This prevents programs from counterfeiting login screens.

Table 2. Generic RACF resource classes (continued)

Class	Function
WRITER	Controls the user of JES2 printers and outbound NJE processing.

The security enforcement of all RACF classes was not subject to evaluation. However, you can choose to use additional classes.

Related concepts

Introduction to the RACF access control module (RACF Access Control Module Guide)

Limiting concurrent sessions for a user

You can define and use a Db2 RACF custom field to provide a limit for a user's concurrent sessions. Db2 uses the value of this field to define the maximum number of concurrent threads for the primary authorization ID of the current ACEE when the COMCRIT subsystem parameter is set to YES.

About this task

A RACF administrator or user who is authorized to define custom fields and add or update data in a custom field can complete this task.

Procedure

To define the maximum number of concurrent sessions for a user ID:

1. Issue the RDEFINE command to define the new custom field USER.CSDATA.DSNMUCTL with the following attributes:

```
RDEFINE CFIELD USER.CSDATA.DSNMUCTL UACC(NONE)
        CFDEF(TYPE(NUM)
        MAXLENGTH(4)
         MINVALUE(0)
        MAXVALUE(2000)
        HELP('DB2 MAX USER CONCURRENT THREAD LIMIT, 4 DIGITS')
        LISTHEAD('DB2 MAX USER THREAD LIMIT='))
```

   The maximum value for this field is 2000 because Db2 allows a maximum of 2000 concurrent threads.
2. Issue the RLIST command to list the new custom field and review the results of the RDEFINE processing:

```
RLIST CFIELD USER.CSDATA.DSNMUCTL CFDEF NORACF
```

3. Add custom field data to the CSDATA segment of a user or group profile by issuing the following command, where *USERABC* is the user ID or group ID and *nnnn* is the maximum number of concurrent threads.:

```
ALTUSER USERABC CSDATA(DSNMUCTL(nnnn))
```

4. Issue the LISTUSER or LISTGRP command to review the contents of the CSDATA segment for the changed user or group profile:

```
LISTUSER USERABC CSDATA NORACF
```

Results

If the USER.CSDATA.DSNMUCTL custom field is not associated with a primary authorization ID in RACF, there is no limit on the number of concurrent sessions for that user ID.

Only new sessions that start while the COMCRIT subsystem parameter is set to YES are counted toward the number of concurrent sessions for a user ID.

Access control

z/OS provides the Resource Access Control Facility (RACF) as the component that performs access control between subjects that act on behalf of a user and resources that are protected by the discretionary and mandatory access control policies.

RACF checks only for authorization to DSNDB04. It does not check for authorization to the implicitly created database.

The protection philosophy of RACF is based on “profiles” that represent protected resources, users, and groups. RACF uses user and resource profiles that it stores in the RACF database to determine if a user has access to a non-UNIX resource (For UNIX resources, the access permissions are carried with the resource itself). For applicable privileges, RACF looks for a match on schema name before checking RACF profiles.

Profiles are organized in profile classes, where each class represents a type of resource (such as data sets or terminals) or other entity (such as users or groups). A profile stores attributes of the subject or object that it represents. For profiles that represent a protected resource, you can assign an access list. This access list specifies the type of access that subjects can have to the resource that is represented by the profile.

Access to Db2 objects is also controlled by RACF. Db2 acts as a resource manager for those objects and calls RACF when a user attempts to access one of those objects. A set of Db2-specific classes are defined in RACF, and profiles in those classes are used to protect the Db2 resources.

Labeled Security only: Db2 uses RACF for row-level security to check the right of the user to access a field in a row, based on the labels for mandatory access control. RACF checks if the current security label of the user allows the type of access, based on the security label of the row and the rules of mandatory access control.

RACF-controlled access is available only at the table and view level (not at the row level) as the lowest granularity of discretionary access.

Related concepts

Authorization checking for implicitly created databases (RACF Access Control Module Guide)

Matching schema names (RACF Access Control Module Guide)

Related reference

Schema privileges (RACF Access Control Module Guide)

Data sets

You must use RACF to protect all data sets in the evaluated configuration.

By default, RACF expects a data set name (and the data set profile name) to consist of at least two qualifiers. RACF also expects the high-level qualifier of the data set profile name to be either a RACF-defined user ID or a RACF-defined group name. If you choose to define data set profiles under the standard RACF naming conventions, you can create a group for each high-level qualifier that is not a user ID. You can also permit users to protect any data set that has that high-level qualifier by giving them CREATE authority in that group.

An installation can use the RACF naming convention table to set up and enforce a data set naming convention other than the convention that is used by RACF. The table can do the following tasks:

- Supply a qualifier that is to be used as the high-level qualifier for authorization checking
- Convert data set names to RACF naming convention form for RACF use
- Convert names in RACF form to the installation-specific format for external display
- Enforce a naming convention by not allowing the definition of data sets that do not conform to the rules of an installation
- Reduce RACF overhead by determining whether a data set is a user data set or group data set

You can create a naming convention table (module ICHNCV00), which RACF uses to check and modify (internally to RACF) the data set name in all commands and macros that process data set names. An

installation can use the table to selectively rearrange data set names to fit the RACF convention without actually changing those names.

If you need to protect data sets that have names consisting of a single qualifier, you can RACF-protect those data sets by issuing the SETROPTS command with the PREFIX operand.

User data sets
A user data set is a data set whose high-level qualifier is a RACF user ID.

The following rules apply to user data sets:

- In general, all RACF-defined users can protect their own data sets.
- A user can RACF-protect a data set for another user under any of the following conditions:
  - The user who is protecting the data set has the SPECIAL attribute. The user can create a discrete or generic profile.
  - The user who is protecting the data set has the group-SPECIAL attribute, and the high-level-qualifier of the data set name is a user within the group-SPECIAL user's scope of authority. The user can create a discrete or generic profile.
  - The user who is protecting a data set has the OPERATIONS attribute (or the group-OPERATIONS attribute if the data set is within the user's scope of authority) and is simultaneously creating the data set. In this case, the user can create a discrete profile by using one of the following methods:
    - Use ADSP.
    - Specify the PROTECT operand on the TSO ALLOCATE command that creates the data set.
    - Specify the PROTECT=YES OR SECMODEL=*profile-name* operands on the JCL DD statement that creates the data set.

Group data sets
A group data set is a data set whose high-level qualifier is a RACF group name.

A RACF-defined user can RACF-protect a group data set under any of the following conditions:

- The user has JOIN, CONNECT, or CREATE authority in the group.
- The user has the SPECIAL attribute (or the group-SPECIAL attribute for that group), and the request is made using the ADDSD command.
- The user has the OPERATIONS attribute and is not connected to the group.

New data sets
By using data set profiles, you can control whether users can create new data sets.

For cataloged data sets, creating, deleting, or renaming the data set involves access not only to the data set profile that protects the data set, but also to the catalog in which the data set is cataloged. In general, users need the following access:

- To add entries to the catalog, users need authority to create the data set as specified below and UPDATE authority to the catalog.
- To delete entries from the catalog, users need ALTER authority to the protecting profile or to the catalog.

A user can create a new user data set in any of the following situations:

- The data set is protected by an existing generic profile, and the user does not have ADSP. RACF allows the user to create a new data set if at least one of the following statements is true:
  - The user has ALTER authority to the data set either through a generic profile or global access checking.
  - The data set is the user's own data set.
- The data set name is not associated with an existing generic profile, the user does not have ADSP, and the data set is protected by the global access check table.

- The user has ADSP, and the data set is the user's own data set. RACF allows the user to create a new data set and creates a discrete profile for the data set.
- The user has the OPERATIONS attribute. If the user has the group-OPERATIONS attribute (that is, the user is connected to a group with the OPERATIONS attribute), the high-level qualifier of the new data set must be the ID of a user who is within the scope of that group.

A user can create a new group data set in any of the following situations:

- The data set name is protected by an existing generic profile, and the user does not have ADSP. RACF allows the user to create a new data set if at least one of the following statements is true:
  - The user has ALTER authority to the data set either through the generic profile or global access checking.
  - The user has CREATE authority in the group.
- The data set name is not associated with an existing generic profile, and the user does not have ADSP.
- The user has ADSP, and the data set belongs to a group of which the user is a member. RACF allows the user to create a new group data set only if the user has CREATE authority in the group. If RACF allows the user to create a new group data set, RACF creates a discrete profile for the data set.
- The user has the OPERATIONS attribute, unless both of the following statements are true:
  - The user is connected to the group with less than CREATE authority.
  - The user has less than ALTER access to the data set if it is protected by a generic profile.

  If the user has the group-OPERATIONS attribute (that is, the user is connected to a superior group with the OPERATIONS attribute), the group for which the new data set is being created must be within the scope of that superior group.

Data set profile ownership
Each data set profile that is defined to RACF requires a RACF-defined user or group as the owner of the profile.

If the owner is a user, the owner has full control over the profile, including the access list.

If the owner of the data set profile is a group, users with group-SPECIAL in that group have full control over the profile.

Ownership of data set profiles is assigned when the profiles are defined to RACF but can be changed later. Ownership of a data set profile does not mean that the owner can automatically access that data set. To access a data set, the owner must still be authorized by the discretionary access control policy rules.

Labeled Security only: The owner must also be authorized by the mandatory access control policy rules to access a data set.

For more information about discretionary access control, see "Discretionary access control" on page 30. For more information about mandatory access control, see "Mandatory access control (Labeled Security only)" on page 28.

Disk and tape volumes

By defining profiles in the DASDVOL class, you can define non-SMS-managed disk volumes to RACF and authorize users to perform maintenance operations (such as dump, restore, scratch, and rename) without giving them access to the data set profiles that protect the data sets on the volume.

If a user does not have the necessary DASDVOL authority to a non-SMS-managed volume, the user must have the necessary authority in the DATASET class for each of the data sets on the volume.

Tape volumes are protected by profiles in the TAPEVOL class.

Devices

A user who is authorized to define profiles in the DEVICES class can use this class to control which users can allocate unit record devices, teleprocessing or communications devices, and graphics devices.

For example, the DEVICES class can be used to ensure that only authorized users can allocate devices by name. The DEVICES class cannot be used to protect other kinds of devices, such as tape or disk devices.

TCP/IP communication

TCP/IP is a component of the IBM Communications Server subsystem of the evaluated configuration. TCP/IP runs as a started task and provides the TCP function in the evaluated configuration.

TCP/IP loads an INET Physical File System into the UNIX System Services kernel to handle socket requests. TCP/IP connects to the VTAM®® component of the Communications Server subsystem of the evaluated configuration for physical communications device management services. Up to eight instances of the TCP/IP started task can be run concurrently on one instance of the evaluated configuration to isolate networks or stacks by security label. Socket applications can be directed to a particular stack or can transparently span multiple stacks. Several TCP/IP resources can be protected by resources in the SERVAUTH class:

- Access to a particular TCP/IP stack is controlled when an application opens a socket by read access to a profile in the following form:

  ```
  EZB.STACKACCESS.system-name.stack-name
  ```

  The *system-name* is the name of the evaluated configuration image, and the *stack-name* is the job name of the particular stack.
- Access to a particular IP address is controlled when an application explicitly binds a socket to a local address and when an application sends data to or receives data from a peer address. IP addresses are configured into named security zones within the stack through use of NETACCESS profile statements. Access to a particular security zone is controlled by read access to a profile in the following form:

  ```
  EZB.NETACCESS.system-name.stack-name.zone-name
  ```

  The *system-name* is the name of the evaluated configuration image, the *stack-name* is the job name of the particular stack, and the *zone-name* is the name of the security zone that contains the IP address.
- Access to a particular port is controlled when an application explicitly binds a socket to a local port. Applications that bind to low ports (below 1024) must be a UNIX superuser or APF-authorized. Port usage can also be controlled by configuring the Port statement in the TCP/IP profile. Control can be controlled by using user ID, job name, or read access to a profile in the following form:

  ```
  EZB.PORTACCESS.system-name.stack-name.SAF-name
  ```

  The *system-name* is the name of the evaluated configuration image, the *stack-name* is the job name of the particular stack, and the *SAF-name* is the name that is configured on the port statement.

(Labeled Security only): TCP/IP performs additional access control when the RACF option MLACTIVE is set. All profiles in the SERVAUTH class require security labels to be defined. Sockets are always considered to be read/write objects; therefore all checks on SERVAUTH profiles require equivalent security labels.

- The security label on the STACKACCESS profile must be identical to the security label of the stack job. Only applications that run under an equivalent security label can access a given stack. A stack that runs under the SYSMULTI label can be accessed by applications with any security label, but communications are allowed only between applications with equivalent security labels.
- The security label on the NETACCESS profile for each local interface address must be identical to the security label of the stack job. This requirement ensures that all implicit address assignments are equivalent to the application security label.
- The security label on the NETACCESS profile for each local VIPA must be equivalent to the stack security label of the stack job and can be SYSMULTI only when the stack job is also SYSMULTI. When

SourceVIPA processing is enabled, a VIPA with a security label that is equivalent to the application is chosen as the implicit source address.

- Communications are permitted only when the source IP address and the destination IP address are in NETACCESS security zones with equivalent security labels. Additionally, when both security zones have SYSMULTI labels, the security label of the sending application is recorded in the IP header in a proprietary format. These proprietary packets are restricted to IUTSAMEHOST links between stacks on the same evaluated system or XCF links between stacks on the same Sysplex.

Mandatory access control (Labeled Security only)

Mandatory access control evaluates dominance and controls user access to information according to the access rules.

Mandatory access control prevents users from accessing information that they do not have clearance to access. It also prevents users from declassifying information by disallowing a user to write to an object unless the security label of the user and the security label of the object are equivalent. Mandatory access is controlled by the Db2 interface with RACF in a Common Criteria-configured system.

To immediately reflect changes in the security policy, long-running applications that have not been committed or rolled back need to be canceled.

Related concepts

Protecting Db2 objects (RACF Access Control Module Guide)

Related reference

Implementing multilevel security with Db2 (Managing Security)

RACF configuration for mandatory access control

In an approved Common Criteria configuration, access control is performed by RACF, not Db2.

To avoid a mix of access control by RACF and access control by Db2, disable Db2 authorization control by defining a profile with the name ** with UACC(NONE) in each of the Db2-related classes. Using these generic profiles ensures that RACF returns either a YES or NO decision when an access request is made. Security is completely controlled by RACF in a Common Criteria-certified configuration.

In RACF, you need to set the value of &ERROPT to 2, which prevents Db2 from using the default Db2 access control if one of the following situations occurs:

- An error occurs during initialization of RACF.
- RACF abends continually.
- Db2 receives an unexpected return code from RACF.

Related concepts

Introduction to the RACF access control module (RACF Access Control Module Guide)

Mandatory access control in z/OS

You can choose to protect objects by using label-based mandatory access control, which is supported by z/OS in the evaluated configuration.

You can define the values for the security levels and the categories. You can then define resources in the SECLABEL resource class as a combination of one security level and zero or more security categories. Such a resource is called a *security label*.

The system defines a set of predefined security labels:

SYSHIGH
Consists of the highest security level and all categories that are defined for the system.

SYSLOW
Consists of the lowest security level that is defined for the system and no categories.

SYSNONE
Is used for resources that need to be read and written by users with different security labels. Reserve this label for resources that can be accessed only in a controlled way using trusted programs to avoid a breach of the information flow policy.

SYSMULTI
Is used for resources that support a range of security labels. Reserve this label for resources that are controlled by trusted programs.

Assign the SYSMULTI security label only to administrators that need to create objects with a SYSMULTI security label.

z/OS prohibits the modification of a security label of a resource unless the system is in a state that allows the activity to be performed in a secure way. This prohibits unauthorized flow of information that might result when users use a resource while the security label of the resource is changed.

The following types of resources have been evaluated with regard to mandatory access control:

- Data sets
- Volumes (DASD and tape)
- TCP/IP connections
- Operator commands

You can choose to apply mandatory access control to other objects also. However, the effectiveness of their protection has not been evaluated.

You can restrict the security labels that can be used with terminals, IP addresses, and devices such as printers. Such restrictions allow the installation to restrict user logons to certain terminals or IP addresses, or to restrict printer output with critical security labels to certain printers.

You can choose to grant the write-down privilege to authorized users on a system that has implemented mandatory access control by using the IRR.WRITEDOWN.BYUSER profile in the FACILITY class.

Mandatory access control in Db2

You can take advantage of mandatory access control in Db2 to protect table data, based on the security labels of the rows.

You must define a column for the security label in the table that you want to protect with mandatory access control by using the AS SECURITY LABEL operand in the CREATE TABLE SQL statement **(Labeled Security only)**.

When a user accesses a row or a field in the row with an SQL statement, Db2 calls RACF to verify that the user is allowed to perform the type of access that is required for the SQL statement. The access is allowed only if the user has the requested access right to all of the rows containing fields that are accessed as part of the SQL statement. For all fields that the SQL statement accesses, Db2 checks the security label of the row containing the field and denies access when the user's security label does not dominate the security label of the any one of the rows containing the fields.

When the system is configured with the RACF MLS option not active, access to Db2 objects, privileges, or administrative authorities is allowed if the user or group that is requesting access is in the access list of the RACF profile that is protecting the object, privilege, or authority with at least READ access.

If the system is configured with the RACF MLS option active, the level of access that is required is UPDATE rather than READ. Use of UPDATE access, regardless of the configuration, rather than READ access in one configuration and UPDATE access in another configuration has no effect on access protection and eases administration.

The security label of a row is initialized with the security label when you create the row using an INSERT SQL statement. Avoid use of the national characters (such as @ # $) in security labels and authorization IDs. If you have the write-down privilege, you can specify a different label than your current one when you create a row. Your security label must dominate the security label that you specify, and you must be authorized to use the security label that you specify.

A user with the write-down privilege can change the security label of an existing row in a table by using an UPDATE SQL statement.

Because the security labels of rows of a Db2 table are stored in a dedicated column of the table, the security labels are exported when the database is exported. The system that imports the labelled data must have defined security labels that are compatible with those of the exporting system to allow the consistent interpretation of the labels.

Related reference

z/OS multilevel security and the Common Criteria (Planning for Multilevel Security and the Common Criteria)

Discretionary access control

Discretionary access control is controlled by RACF.

Db2 internal access controls, which are the GRANT and REVOKE statements, are not used in the evaluated configuration.

If you use mandatory access control, discretionary access control occurs after mandatory access control is complete **(Labeled Security only)**.

Related concepts

Protecting Db2 objects (RACF Access Control Module Guide)

Related reference

Implementing multilevel security with Db2 (Managing Security)

Discretionary access control in z/OS

Discretionary access control to RACF resources is controlled by the user, group, and resource profiles that are stored and managed by RACF.

RACF controls the types of access to all non-UNIX resources with access lists. The access types are ordered hierarchically, an access type that is listed higher in the access hierarchy implies that it has all of the access types lower in this hierarchy except for NONE access. The semantics of the access types might differ depending on the resource class. The full semantics of each access type are defined by the resource manager.

You can control access to resources by using discrete resource profiles for a specific resource or generic resource profiles for a set of resources of the same type. Discrete profiles protect one single resource (such as one data set), whereas generic profiles can be used to define a whole set of resources and protect them using a single profile that is based on patterns in the resource name. Whenever a discrete profile exists for a resource, it has precedence over a generic profile that also would apply for the resource. If more than one generic profile applies, z/OS always chooses the most specific profile that is applicable based on a matching algorithm.

Related reference

RACF commands (Security Server RACF Command Language Reference)

RACF security administration (Security Server RACF Security Administrator's Guide)

Discretionary access control in Db2

Discretionary access control is defined for Db2 objects.

Each Db2 command, utility, and SQL statement is associated with a set of privileges, authorities, or both. Authority control is performed with the support of the RACF access control module. Db2 authority checking ensures that Db2 objects map to RACF objects such that the following statements are all true:

- Db2 object types map to RACF class names.
- Db2 privileges map to RACF resource names for Db2 objects.
- Db2 authorities map to the RACF administrative authority class (DSNADM) and to the RACF resource.
- Db2 security rules map to RACF profiles.

Rows are not objects that are subject to discretionary access control on their own. Discretionary access control is at the granularity of a table or a column.

When the system is configured with the RACF MLS option not active, access to Db2 objects, privileges, or administrative authorities is allowed if the user or group that is requesting access is in the access list of the RACF profile that is protecting the object, privilege, or authority with at least READ access.

If the system is configured with the RACF MLS option active, the level of access that is required is UPDATE rather than READ. Use of UPDATE access, regardless of the configuration, rather than READ access in one configuration and UPDATE access in another configuration has no effect on access protection and eases administration.

Related reference

z/OS multilevel security and the Common Criteria (Planning for Multilevel Security and the Common Criteria)

z/OS users and groups

z/OS users and groups are defined in RACF.

User roles and attributes are capabilities, restrictions, or environments that can be assigned to a user, either all of the time or when the user is connected to a specific group or groups. User attributes are stored and managed within the RACF database.

When a role or attribute applies only to a specific group or groups, it is specified at the group level and is called a group-related user attribute.

For example, user attributes that are specified in an ADDUSER or ALTUSER command are stored in the user's profile and are in effect regardless of the group to which the user is connected.

Creation of user profiles

To create user profiles and user attributes, create RACF user profiles. Users can be people or programs.

To create a user profile, create a user profile for the new user in RACF. Each user profile consists of a base segment and optional segments for the use of specific subsystems. In the evaluated configuration, the user attributes that the evaluated configuration requires are contained in the base segment and the OMVS segment for z/OS UNIX System Services. Other segments of the user profile might exist, but the effects of any values in those segments do not influence the security of the evaluated configuration.

To create or modify a user profile, a user must be authorized in one of the following ways:

- Has SPECIAL role as a general system administrator.
- Has UPDATE authority to the fields in a non-base segment of the profile that the user wants to modify through field-level access checking.
- Create user profile only: Is connected to a user that has the group-SPECIAL role, has the CLAUTH attribute for the USER class, and is the owner of or has JOIN authority in the new user's default group.

  The following roles of the ADDUSER command cannot be assigned in this case:

  – OPERATIONS
  – SPECIAL
  – AUDITOR
- Modify user profile only: Has the CLAUTH attribute for the user class. Only the CLAUTH and NOCLAUTH attributes can be changed.

Creation of group profiles

To make the management of users, user attributes, and roles easier, you can define groups of RACF users in group profiles.

To create a new group of users, define a group profile in RACF. A group profile (like a user profile) consists of a base segment and, optionally, other segments. As with user profiles, all group attributes that the

evaluated configuration requires are contained in the base segment and in the OMVS segment of the group profile. Each group that is defined in RACF must be owned by a RACF-defined user or by its superior group. You can assign ownership of a group with the ADDGROUP command when you create a new group profile. You can change ownership of a group with the ALTGROUP command when you change an existing group profile.

The owner of a group or a user who has the group-SPECIAL role and is connected to a group can perform the following actions:

- Define new users to RACF (if the user also has the CLAUTH attribute for the USER class)
- Connect and remove users from the group
- Delegate and change group authorities and set the default UACC for all new resources that belong to members of the group
- Modify, list, and delete the group profile
- Define, delete, and list the names of the subgroups under the group
- Specify the group terminal option

Users can be connected to a number of groups and have the group-related authorities of all the groups that they are connected to. The OMVS segment of a group profile contains the group's z/OS UNIX group identifier.

z/OS user roles

You can choose to grant the AUDITOR privilege only to users who do not have the SPECIAL privilege.

Recommendation: Keep user privileges such as the SPECIAL or OPERATIONS user attributes under control, and assign these attributes based on operational needs.

Db2 user roles

Db2 user roles, which are also known as Db2 administrative authorities, are defined by dedicated profiles in the DSNADM class.

When a user is assigned access to a profile that is associated with a role, the user is also assigned that role. This assignment can be done by any user that is allowed to assign permission to those profiles according to the rules that are implemented in RACF.

Db2 supports the following roles:

- ACCESSCTRL
- DATAACCESS
- DBADM
- DBCTRL
- DBMAINT
- Installation SYSADM
- Installation SYSOPR
- PACKADM
- SECADM
- SQLADM
- SYSADM
- SYSCTRL
- SYSDBADM
- SYSOPR

SYSADM, SYSCTRL, and SYSOPR are roles with privileges on the Db2 subsystem level. DBADM, DBCTRL, and DBMAINT are roles with privileges on the database level within a defined Db2 subsystem. PACKADM is a role that is defined on the level of a collection.

Installation SYSADM and installation SYSOPR are roles that are used for the initial setup and configuration of Db2. In the evaluated configuration, these roles must be disabled after the initial configuration.

Security-related audits

The evaluated configuration provides a general facility to collect data that is required for security-related auditing information. This facility, the System Management Facility (SMF), collects and records system- and job-related information that you can use.

RACF generates both audit records that are related to access control checking for Db2 objects and audit records that are related to access control checking of other objects that are protected by RACF. You can define what is audited with the AUDIT parameter of the ADDSD, ALTDSD, RDEFINE, and RALTER commands or with the GLOBALAUDIT parameter of the ALTDSD and RALTER commands.

Db2 generates audit records for security-relevant audit data by using the Db2 trace facility. You can use the START TRACE command to start the generation of audit trace records and the STOP TRACE command to stop the generation of Db2-related audit records. The trace must be directed to SMF so that the protection functions of SMF apply.

Audit data protection

You must take steps to protect SMF data sets and dump data sets.

SMF writes audit records into dedicated SMF data sets that you define during system configuration. The evaluated configuration requires that you define at least two SMF data sets. You must protect the SMF data sets and dump data sets against unauthorized access by using RACF access control lists. The evaluated configuration requires that the system halts if no buffer space is available for the SMF audit records.

Db2 audit trace records are also stored by SMF and protected by RACF access control lists.

Malfunction such as a power loss can affect the consistency of the audit records.

Object reuse

You must prepare objects for reuse.

z/OS supports explicit object reuse for the following objects:

- Memory objects
- z/OS data sets
- z/OS tape volumes

In the evaluated configuration, z/OS ensures that objects are prepared for reuse before they are allocated to another subject. Memory objects are filled with zeros before they are allocated for the first time to a subject. DASD data from z/OS data sets is erased when the data is released when the erase-on-scratch option is active. Tape volumes are erased when they are returned to the scratch pool by appropriately configuring the SECCLS PARMLIB option for the PARMLIB member EDGRMMxx. z/OS UNIX file system objects and z/OS UNIX IPC objects are cleared before they are made accessible to a new user.

The evaluated parts of Db2 execute in their own address spaces. Object reuse of memory objects within those address spaces is provided by z/OS functions.

Db2 manages its own objects. When a Db2 object is deleted, Db2 ensures that the space that has been occupied by that object cannot be accessed by Db2 unless the space is allocated to another Db2 object and completely filled with the initial values for the new object. This ensures that values that are stored in space that is allocated to Db2 objects that have been deleted cannot be accessed by Db2 until the space is allocated to another Db2 object and has been prepared for reuse as part of the allocation.

Db2 stores its objects in z/OS data sets. Object reuse for data sets is provided by z/OS. RACF access control functions for data sets prohibit direct access by untrusted users to the data sets that are used by Db2.

Chapter 6. Common Criteria resources

For general information about Common Criteria, refer to the following Web site: `http://www.commoncriteriaportal.org/`

© Copyright IBM Corp. 2007, 2017

Information resources for Db2 11 for z/OS and related products

Information about Db2 11 for z/OS and products that you might use in conjunction with Db2 11 is available online in .

You can find the complete set of product documentation for Db2 11 for z/OS in IBM Knowledge Center.

You can also download other PDF format manuals for Db2 11 for z/OS from in PDF format manuals for Db2 11 for z/OS (Db2 Home).

© Copyright IBM Corp. 2007, 2017

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785 US

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785 US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

© Copyright IBM Corp. 2007, 2017

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as shown below:

© (*your company name*) (*year*).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. (*enter the year or years*).

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming interface information

This information describes the Common Criteria-evaluated version of Db2 11 for z/OS servers. This information also documents Product-sensitive Programming Interface and Associated Guidance Information provided by Db2 11 for z/OS.

Product-sensitive Programming Interface and Associated Guidance Information

Product-sensitive Programming Interfaces allow the customer installation to perform tasks such as diagnosing, modifying, monitoring, repairing, tailoring, or tuning of this IBM software product. Use of such interfaces creates dependencies on the detailed design or implementation of the IBM software product. Product-sensitive Programming Interfaces should be used only for these specialized purposes. Because of their dependencies on detailed design and implementation, it is to be expected that programs written to such interfaces may need to be changed in order to run with new product releases or versions, or as a result of service.

Product-sensitive Programming Interface and Associated Guidance Information is identified where it occurs by the following markings:

PSPI Product-sensitive Programming Interface and Associated Guidance Information... PSPI

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered marks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at: http://www.ibm.com/legal/copytrade.shtml.

Linux® is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions:

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

Personal use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights: Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Glossary

The glossary is available in IBM Knowledge Center.

See the Glossary topic for definitions of Db2 for z/OS terms.

© Copyright IBM Corp. 2007, 2017

Index

A

access control
  discretionary 30
  mandatory 28
accessibility
  keyboard vi
  shortcut keys vi
administrative authorities 32
audit data protection 33
auditing 33
authentication 19

C

Common Criteria
  resources 35
  Web site 35
Common Criteria-evaluated configuration v
concurrent sessions 23
configuration
  hardware 7
  RACF password 19
  system 19
connections to Db2 5
Controlled Access 1
create group profiles 31
create user profiles 31
CSDATA segment 23

D

DASD volumes 26
data set profile ownership 26
data sets
  group 25
  new 25
  user 25
Db2 for z/OS 1
Db2 installation 9
Db2 user roles 32
devices 27
disability vi
disabling
  installation SYSADM 16
  installation SYSOPR 16
discretionary access control
  Db2 30
  description 30
  z/OS 30

E

evaluated configuration software 11

G

group data sets 25
groups
  create profiles 31
  z/OS 31

H

hardware configuration 7

I

IBM Z hardware 7
identification 19
installation
  evaluated configuration 9
  options 12
  restrictions 12
  z/OS 12
installation SYSADM 16
installation SYSOPR 16
ISO standard 1

L

Labeled Security 1
limit threads 23
links
  non-IBM Web sites 41

M

mandatory access control
  Db2 29
  RACF configuration 28
  z/OS 28

N

new data sets 25

O

objects
  reuse 33
operational environment 3
organizational security policy 3

P

peripheral 7
personnel requirements 4
physical security 4
procedural requirements 5

product-sensitive programming information, described 40
profiles
    RACF 24
programming interface information, described 40
PSPI symbols 40

R

RACF
    configuration 20
    configuration for mandatory access control 28
    options 20
    profiles 24
    resource classes 20
RACF password configuration 19

S

security environment 3
security objectives
    IT 3
    non-IT 3, 4
SETROPTS 20
shortcut keys
    keyboard vi
SMF 33
system configuration 19
System Management Facility (SMF) 33

T

TCP/IP communication 27
threats to Db2 5

U

user data sets 25
user roles
    Db2 32
    z/OS 32
USER.CSDATA.DSNMUCTL field 23
users
    create profiles 31
    z/OS 31
users and groups 31

Z

z/OS 1
z/OS installation 12
z/OS user roles 32



Product Number: 5615-DB2
5697-P43

SC19-4011

