Draft Document for Review November 28, 2023 9:22 am SG24-5677-01

Redbooks
ibm.com/redbooks

Broadcom Top Secret and z/OS Security Server

Bill Samsoe

Dan Brunton

Security

IBM Z

IBM

Redbooks

IBM Redbooks

Broadcom Top Secret and z/OS Security Server

November 2023

Note: Before using this information and the product it supports, read the information in , “Notices” on page ix.

Second Edition (November 2023)

This edition applies to SecureWay Security Server Version 2, Release Number 10, Program Number 5645-001 for use with the z/OS Operating System

Contents

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 grant 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

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 provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, 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 https://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

CICS®
Db2®
IBM®
IBM Security®
IBM z16™
OS/390®
RACF®
Redbooks®
Redbooks (logo) ®
Tivoli®
VTAM®
z/OS®
z16™

The following terms are trademarks of other companies:

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

Other company, product, or service names may be trademarks or service marks of others.

Preface

Broadcom Top Secret and the IBM® z/OS® Security Server (RACF®) are both Mainframe Security products. In some areas their designs are similar, and in other areas the designs are very different. Planning a migration from Broadcom Top Secret to z/OS Security Server RACF, without unduly disrupting an z/OS production environment, requires considerable planning and understanding. With proper planning, and perhaps with specially skilled people to assist in certain areas, the migration can usually be accomplished in an orderly way.

This IBM Redbooks® publication will assist in understanding the higher-level issues and differences between the two products as an important starting point.

The Team That Wrote This Redbook

This Redbook was produced by a team of specialists from around the world working at the IBM Redbooks Poughkeepsie Center.

Bill Samsoe is a Mainframe Security Specialist in the United States. He has 40 years of experience in IT field.

Dan Brunton is a Mainframe Specialist in the United States. He has 40 years of experience in the IT field, 26 years of which with IBM

Thanks to the following people for their contributions to this project:

Lydia Parziale
IBM Redbooks, Poughkeepsie Center

Thanks to the authors of the previous editions of this book.

- Authors of the first edition, CA-TopSecret to OS/390® Security Server Migration Guide:

  Paul de Graaff,Ted Anderson,Julie Bergh,Peter Desforge,Lynn Kearney,Lori Halberts Kikuchi,Tony Nix,Mark Shell

Now you can become a published author, too!

Here’s an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments Welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, IBM Redbooks
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay Connected to IBM Redbooks

- Find us on LinkedIn:

  https://www.linkedin.com/groups/2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/subscribe

- Stay current on recent Redbooks publications with RSS Feeds:

  https://www.redbooks.ibm.com/rss.html

•

1

The Value of IBM z/OS Security Server RACF

This chapter describes the advantages of using the z/OS Security Server RACF versus competitive security software from Broadcom Top Secret. The value is presented both from a functional point of view, component by component, to the monetary savings of the z/OS Security Server.

1.1 Overview of the z/OS Security Server

In 2001 the IBM corporation offered a newly packaged operating system for mainframes, named z/OS, z/OS integrates numerous products, which are pretested, integrated, and packaged together. This integration, performed by IBM, is very beneficial to the users of z/OS because now only one product needs to be ordered: There is no need to test numerous separate products each time an operating system upgrade is performed, and it even costs less. Most of the products packaged in z/OS, like JES2 and IBM VTAM®, became standard features of z/OS. Other products, like z/OS Security Server for RACF and DFSMS, became optional features of z/OS. Both standard and optional features are packaged, tested and delivered with every license of z/OS, but to use the optional features you must order the feature codes from IBM and enable the features on your system.

The design and development of the z/OS Security Server RACF follows a published architecture that adheres to standards. RACF does not modify or front-end any modules nor does it dynamically place hooks into product code. RACF uses the z/OS provided SAF interface. By following standards and using the SAF interface RACF provides reliability and allows for ease of release to release migration. Along with all of this RACF also provides day-1 support for new system technology and new product releases, but it does not stop there, it also exploits these new technologies. When IBM moved from MVS to z/OS there was a perception in the marketplace that the name of RACF had been changed to z/OS Security Server RACF. Actually, z/OS Security Server RACF is more than just a new name for IBM's RACF for z/OS. IBM created a “security umbrella” as a delivery vehicle for IBM z/OS security-oriented software. RACF is but one of the products in the Security Server. In z/OS Security Server RACF, there are six products:

1. DCE Security Server
2. .Lightweight Directory Access Protocol (LDAP) Server
3. z/OS Firewall Technologies
4. .Network Authentication Service for z/OS
5. Enterprise Identity Mapping (EIM)
6. PKI Services

IBM has positioned the z/OS Security Server RACF as the security product that will deliver the support and exploitation of new technology inside the glass house and in the e-business arena.

1.1.1 Business Benefits of the z/OS Security Server RACF

The job of your security product is to protect your information while allowing your business to move ahead with new ventures and technologies. RACF is the leader in this area. RACF integrates seamlessly upon availability of new versions and releases of IBM subsystems (for example, CICS®, Db2®) and technologies (e.g., Sysplex Coupling Facility). This allows your business to move ahead with its objectives and applications as quickly as you choose. Many non-RACF customers have been held back for months by their current mainframe security product.

With the LDAP Protocol Server, IBM continues this tradition outside of the glass house. The z/OS Security Server RACF delivered the LDAP Server as one of its products before many companies even knew about the new Lightweight Directory Access Protocol. Now those same companies are ready to roll out applications and directories that will make use of the LDAP Server on z/OS, and they can do that with the confidence of knowing that the server was delivered as part of the z/OS Security Server RACF -- and it is ready and waiting for them.

Now any authorized LDAP client throughout the enterprise can search, extract, add and delete information from any z/OS LDAP server (from the IBM z/OS Security Server RACF Security Administrator's Guide, SA23-2289-50). See Chapter 2 in section 2.2.4 regarding LDAP.

The Firewall Technology product of the z/OS Security Server delivers a set of features that can be used alone or with the Firewall Technologies that already ship in the z/OS Communications Server, a standard part of the z/OS Operating System. When used together, you have a full function z/OS Firewall ready to use. The Virtual Private Network (IPsec) support of the z/OS Firewall is one of the areas where it excels.

The RACF product of z/OS Security Server 1.4 first introduced support for Digital Certificates and Public Key Infrastructure (PKI), z/OS Security Server RACF 1.8 greatly enhanced that support. Again, RACF has new technology ready and waiting for you to move into the world of e-business. The following is a high-level list of the supported technology features:

- Digital Certificate Authentication providing integration between PKI Technology and traditional RACF Authentication.
- Certificate mapped to RACF user ID, to provide seamless access to z/OS resources.
- User self-registration of digital certificates.
- Processing of certificate revocation lists by the IBM HTTP Server for z/OS.
- RACF can generate digital certificates.

1.1.2 Financial benefits of the z/OS Security Server

There are many scenarios where the value of the z/OS Security Server RACF is evident, not the least of which is the scenario of upgrading CPUs. IBM's pricing policies are flexible yet predictable. There are no surprises regarding huge software upgrade bills.

Identifying productivity savings

The z/OS Security Server RACF is an optional feature of the z/OS operating system. The benefit of being a feature of z/OS is that the Security Server is integrated and pretested with the z/OS operating system. This reduces the amount of testing that your systems staff devotes to your security package. Most of our customers see a substantial time savings each time a new release of the operating system or non-RACF mainframe security product is installed. The savings to your systems programming organization will reflect these savings multiple times per year.

1.2 RACF added features and functions

This section highlights added features and functions to z/OS Security Server RACF and some of the recent administration enhancements made to RACF.

- RACF Database Encryption

  Continuing the pervasive encryption readmit, RACF now supports RACF database encryption. This function allows an installation to encrypt a VSAM data set that is used as a part of a RACF data base as well as share that data set among z/OS systems in certain configurations to help further strengthen the overall security posture of the z/OS platform.

- Compliance support for z/OS

  z/OS has been enhanced to modernize compliance data reporting which enables the collection of compliance data from numerous IBM z16™ and z/OS products and components. z/OS has also simplified auditing by contributing IBM z/OS V2R5 with RACF Benchmark v1.0.0, which provides security best practices and guidance to clients and auditors.

- RACF for z/OS

  Achieved Common Criteria certification at Evaluation Assurance Level 4 (EAL4+) under the Common Criteria Evaluation and Certification Scheme. This certification along with RACF, TCP/IP, UNIX System Services and Db2 provides our customers with a Multilevel security (MLS) solution.

- Support for RACF password phrases by TSO/E logon, z/OS UNIX functions, OpenSSH, and the IBM Tivoli® Directory Server.
- The RACF CFIELD class

  This can be used to create customer defined fields for user, group, dataset and general resource profiles, and the labels you want to use for them.

RACF supports the use of passwords longer than eight characters, often called pass phrases. A pass phrase is a character string that can comprise mixed-case letters, numbers, and special characters including blanks, from 14 to 100 characters in length. Pass phrases allow for an exponentially greater number of possible combinations of characters and numbers than do passwords.

1.2.1 RACF administrative enhancements

Historically, RACF has brought out day-one support and exploitation of new software and hardware technologies. This is beneficial to corporations who like to be on the leading edge with new technology. For example, many customers with RACF have enjoyed the benefits of having RACF make use of the Coupling Facility since day one.

RACF's Remote Sharing Facility (RRSF) is an integrated feature of the RACF product, which allows you to administer and synchronize multiple RACF databases. RRSF is extremely granular which allows you to make the choices that fit your business. For example, some or all commands and/or passwords can be synchronized automatically or they can be specifically targeted to one or more of the databases being managed. IBM has delivered this integrated feature with the utmost of integrity by encrypting the transmission of data and by providing automatic recovery if the transmission is interrupted.

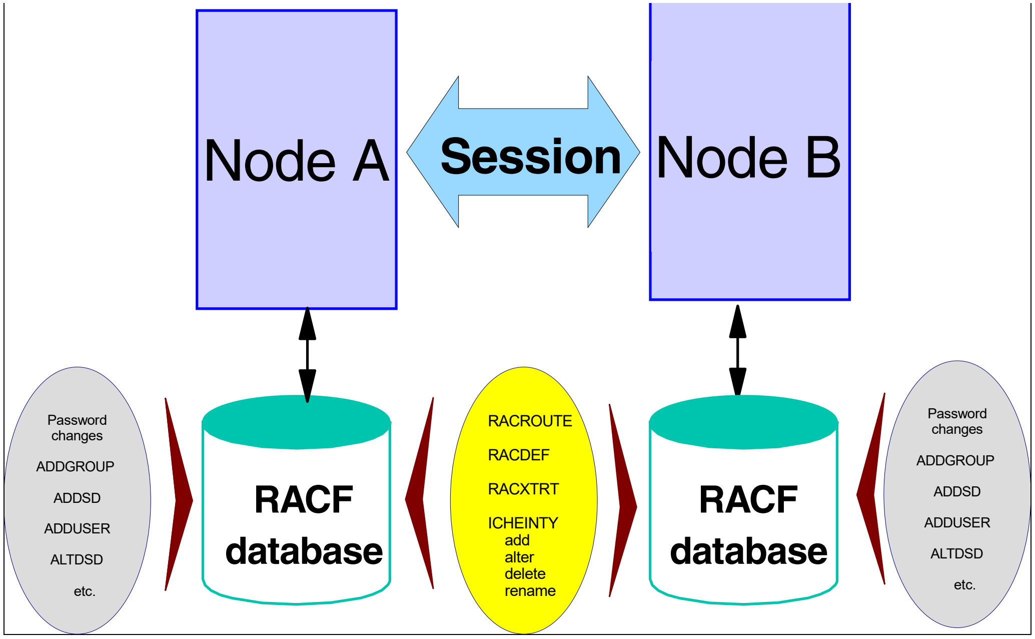


Figure 1-1 RRSF overview

RACF has a number or logging and reporting options that allow a Resource Owner to identify users who attempt to access the resource. In addition, you and your Auditor can use these functions to log all detected successful and unsuccessful attempts to access the RACF DB and any RACF protected resources. Logging all access attempts to detect possible security exposures or threats.

The logging and reporting options are:

- Logging - RACF writes records to the System Management Facility (SMF) for detected, unauthorized attempts to enter the system.
- Access RACF Protected Resources Introduction
- Issue RACF commands
- Modify profiles on the RACF Database, RACF writes these records to an SMF Data Set. To list SMF records, you can use either the RACF SMF Data Unload Utility (IRRADU00) or the RACF Report Writer.
- With the SMF data unload utility, you can translate the RACF SMF records into a format you can browse or upload to a database, query, or reporting package, such as Db2 z/OS.
- With the Report Writer, you can select RACF SMF records to produce the reports. Because the RACF report writer was stabilized at the RACF 1.9.2 level, it cannot produce reports for all records beyond that release. The RACF Report Writer provides a wide range of reports that enable you to monitor and verify the use of the system and resources.
- The RACFICE reporting tool allows an installation to create tailored RACF reports without requiring a relational database management product, and provides an alternative to the RACF report writer. It makes use of the DFSORT ICETOOL reporting facility. RACF makes several ICETOOL-based reports available in SYS1.SAMPLIB. The RACJCL member of SYS1.SAMPLIB provides sample JCL to allocate a report data set and add the RACFICE reports in IEBUPDTE format.

- The Data Security Monitor produces reports on the status of the security environment at your installation and, in particular, on the status of resources that RACF controls. You can use the reports to audit the current status of your installation's system security environment by comparing the actual system characteristics and resource-protection levels with the intended characteristics and levels

Both the Report Writer and DSMON are still supported and shipped with z/OS Security Server RACF. IBM met customer requirements by adding the following two additional reporting options:

1. The RACF Database Unload feature
2. The SMF Unload feature

These features allow you to unload the RACF database and the violation records from SMF into flat files. IBM ships a comprehensive set of Db2 based reporting queries to meet your needs. In addition, you can use any SQL- based language or product to create reports from the flat files. This method of reporting allows you to combine data stores to create more informative trend analysis reports on a user, system, or across platforms.

The RACF product delivered with version 2.8 of z/OS Security Server includes an administrative enhancement for reporting, called RACFICE, which was formerly only available via the Web. This feature includes numerous sample reports, and it uses the DFDSS ICETOOL report generator. This is very beneficial to organizations that do not have Db2, and they can now easily make use of the database and SMF Unload utilities without having to write their own queries. Additional reporting options can be found in the IBM product Performance Reporter for z/OS. Performance Reporter includes several canned reports for RACF in its extensive list of performance-related reports.

The RACF Remove ID utility is a helpful feature of RACF that greatly enhances the productivity of security administrators. This utility allows the administrator to search for an occurrence of a user ID or group. The results of the returned search are a set of RACF commands to delete the user ID or Group and its related access permissions. The administrator can then mark the ones to delete, as it may not be appropriate to delete all occurrences. The administrator can then submit the results and the deletions will take place.

1.2.2 RACF/Db2 security administration overview

z/OS Security Server RACF 2.4 introduced the RACF /Db2 Administration Feature with Db2 Version 5. This feature allows security administrators to manage Db2 security administration via RACF. The RACF /Db2 external security module is shipped with the z/OS Security Server.

RACF and Broadcom’s Top Secret have Identification, Authentication and the use of Secondary Authorization IDs in their base support -- this is not the issue. We are comparing the RACF /Db2 external security module to the Broadcom’s Top Secret Db2 add-on product. Using either the Broadcom add-on products or the RACF /Db2 feature you can realize the benefits of moving your Db2 security administration function out of Db2 and into your z/OS security product. Db2 is an outstanding database product, but its internal security structure does not provide the robust level of security administration that most organizations desire. Figure 1-2 on page 9 shows an overview of Db2 external (RACF) Security.

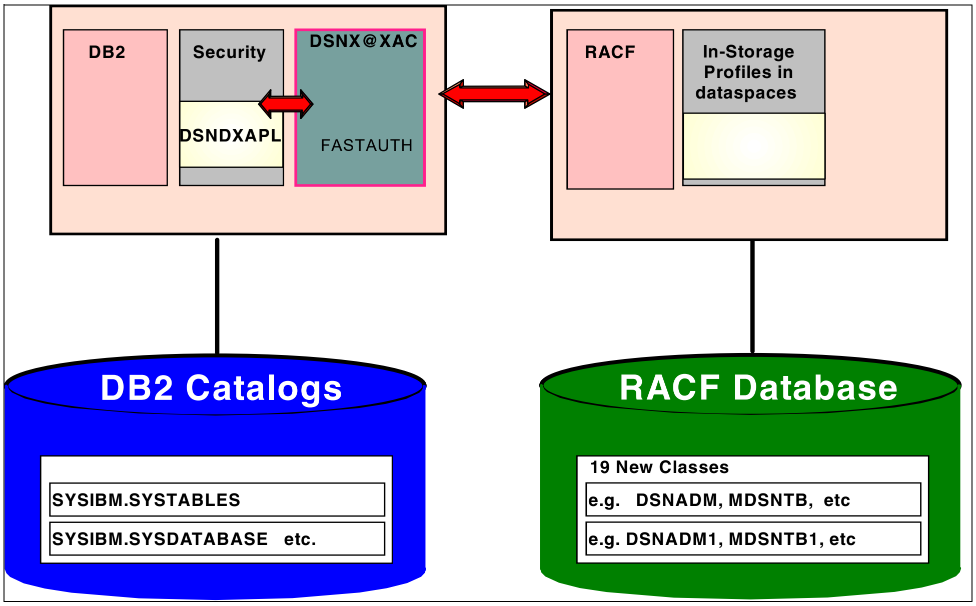


Figure 1-2 Db2 external security (RACF) overview

Benefits of using RACF to administer your Db2 security

The following benefits are gained when you use RACF for Db2 security:

- Separation of duties
- Single point of control for Administration and Auditing
- Ability to define security rules before a Db2 object is created
- Ability to allow security rules to persist when a Db2 object is dropped
- Ability to protect multiple Db2 objects with one security rule
- Eliminate the need to create multiple, and sometimes duplicate, security rules
- Ability to use RACF Generic Profiles and/or Member/Grouping Profiles
- Eliminate Db2 cascading revoke
- Flexibility for multiple Db2 subsystems:
  - One set of RACF Classes for multiple Db2 Subsystems, or
  - One set of RACF Classes for each Db2 Subsystem

Migration issues: Protection of Db2 resources via RACF

For organizations currently using the Broadcom Top Secret/Db2 product, the IBM SMPO Security Team’s migration tools have built-in functions that can convert your Db2 add-on product data into the appropriate RACF commands to provide you with equivalent function via the RACF /Db2 external security model.

For organizations currently using internal Db2 security administration, RACF will allow you to phase in the RACF /Db2 function while you move from internal to external Db2 security administration. Once you have begun protecting Db2 Resources via the RACF external security module, the RACF /Db2 external security module will look at the RACF profiles first. If there is not a RACF Profile to protect the Db2 Object, then the RACF /Db2 external security module passes control to Db2’s internal security authorization catalogs. This allows you to move over to external security in a manner best suited for your organization.

Product benefits

Since the administrative function is included in RACF, there is no additional maintenance that needs to be done. The Broadcom Top Secret solution is delivered in a separate product, so there is an additional product to maintain, upgrade and test.

The external security module is shipped in the SAMPLIB member IRR@XACS. It is coded and fully supported by the IBM RACF development team. This means that you can call the IBM support center if you have any problems with this code, and they will support you and accept APARs if it is determined that a problem does exist.

The external security module is installed in Db2 at the Access Control Authorization Exit point. This allows RACF and Db2 to make use of the standard SAF interface, which eliminates the need to install or modify any Db2 product code. IBM’s implementation of the external security module provides any vendor the ability to perform Db2 security administration within its product without the requirement of modifying or overlaying Db2 code by simply using the industry standard SAF interface.

The IBM RACF development team works in concert with the Db2 development team to make sure that this module works and that it continues to work as each product comes out with new releases and versions. As a user of this function, you can feel confident that you will have day-one support of new releases and versions.

Financial benefits

The RACF/Db2 external security module code is shipped with RACF for use with Db2 V5 and higher at no additional cost. The competitive product, Broadcom’s Top Secret /Db2, is sold as a separate product.

Identifying financial savings based on product price

If you have already purchased this add-on product from Broadcom then you will see an annual savings equal to your current maintenance charges. Most contracts that organizations have negotiated with Broadcom do not have “out” clauses. Therefore, you will probably not realize these savings until the end of the contract period.

If you are trying to cost justify the migration to RACF and currently have funds for the Broadcom Db2 add-on product allocated in your budget, then you can free up all OTC funds and the annual maintenance fee. In most cases, the amount of money that is saved can be used to cover the migration charges for the SMPO’s Security Migration Team to advise and assist you with your migration.

Don’t forget that these Broadcom products will most likely be subject to upgrade charges when your CPU is upgraded or a new CPU is purchased.

Broadcom has purchased Platinum, the company that came out with the RC Secure product. If you are currently using RC Secure, then you may also be able to discontinue that product when you implement the RACF /Db2 function. Once your contract has ended for RC Secure, you will also realize those savings.

Identifying productivity savings

The maintenance effort for RACF is easy to identify and quantify. It should take your systems programmer less than an hour to initially get the RACF /Db2 external security module installed. Annually, this should require minimal maintenance, if any at all.

If you are currently using the Broadcom Db2 add-on product, then you can easily quantify the benefits of migrating to RACF. You will need to quantify the number of hours the systems programming staff expends installing and maintaining this product on an annual basis. Subtract one hour per year from that number and you will arrive at the annual savings in hours that your organization should realize after migrating to RACF.

1.3 RACF market penetration

RACF has been securing data in the z/OS environment for 45 years. Most companies chose their security products in the early 1980's. The main choices then, as now, are RACF from IBM and Broadcom's ACF2 and Top Secret. At that time Computer Associates owned these products until it was acquired by Broadcom. Most organizations chose Broadcom's ACF2 or Top Secret over RACF, because at that time RACF was not an extremely robust product.

Since the early to mid nineties organizations began taking a second look at RACF. Often the initial reason to consider migrating was, and still is, a dissatisfaction with their current vendor. Once these organizations began to research the implications of migrating to RACF, they also saw that RACF had become a robust product. It became very clear that IBM had committed itself to making RACF the best security product on the z/OS operating system.

In 1986 RACF had roughly a 28% market share in the United States. This is based on the number of RACF licenses billed in z/OS environments. RACF was the number three product behind Broadcom's ACF2 and Top Secret.

In 1993 the penetration had grown to approximately 38%, and by 1998 the penetration was 70%. The rise in market share in the United States had finally caught up with the rest of the world and as of 2023 the penetration rates are based on the world-wide penetration of RACF on z/OS systems.

At the end of 1999, the RACF penetration rate had exceeded 100%. Some machines have more than one security product running in separate LPARs. Therefore, the marketplace actually exceeds 100%. We estimate that there is probably a 110% penetrated market, meaning that RACF is licensed on over 70% of z/OS licenses. The remaining 40% or so of the market is shared between Broadcom's Top Secret and ACF2.

Since so many migrations have taken place in just the past twenty-five years, Broadcom may still be receiving a revenue stream on unused licenses due to their practice of long-term contracts. This could mean that internally they show a higher penetration.

Many organizations are confused when we tell them that RACF has such a high penetration rate, and that it is the top security product in the z/OS arena. The reason for this confusion lies with understanding the basis for the penetration rates that are quoted by various vendors. Be sure to ask other vendors how many operating systems and how many products are included in their penetration number. Remember, IBM's penetration rate only includes actual revenue producing licenses only on the z/OS operating systems

2

z/OS Security Server RACF

IBM z/OS Security Server RACF software is an optional feature of z/OS that lets you control access to protected resources and provides integrated directory, connectivity, and security between users and applications for e-business in a networked world. Every e-commerce application requires the ability to: locate resources, such as people, information and applications in the network; connect customers, partners, and employees to those resources across multiple systems; address the concern about how to secure communications, data, and transactions. z/OS Security Server integrates these infrastructure requirements to provide the Secure Network Platform needed for e-business. IBM Security® Server software is supported on multiple platforms, including z/OS.
This chapter provides a high-level overview of the z/OS Security Server RACF and the security enhancements of the IBM Communication Server for z/OS.

2.1 Introduction to the z/OS Security Server RACF

Advances in the use of, and general familiarity with, small computers and data processing have increased the need for data security. IBM incorporates the z/OS Security Server RACF, which provides a platform that gives you solid security for your entire enterprise, including support for the latest technologies. As a feature of z/OS, the z/OS Security Server comes with the major components described in the following sections.

2.1.1 Resource Access Control Facility (RACF)

The primary component of the z/OS Security Server is the Resource Access Control Facility (RACF). RACF works closely with z/OS to protect its vital resources. Building from a strong security base provided by the RACF component, the z/OS Security Server RACF is able to incorporate additional components that aid in securing your system as you make your business data and applications accessible by your intranet, extranets, or the Internet.

Using an entity known as the RACF user ID, RACF can identify users requesting access to the system. The RACF user Password (or valid substitute, such as RACF PassTickets or Digital certificate) authenticates the RACF user ID. RACF supports the use of PassTickets as other products use this to present a single sign-on environment to end users at their workstations. Once a user is authenticated, RACF and the resource managers control the interaction between that user and the objects it tries to gain access to. Figure 2-1 on page 14 shows an overview of RACF and its functions.

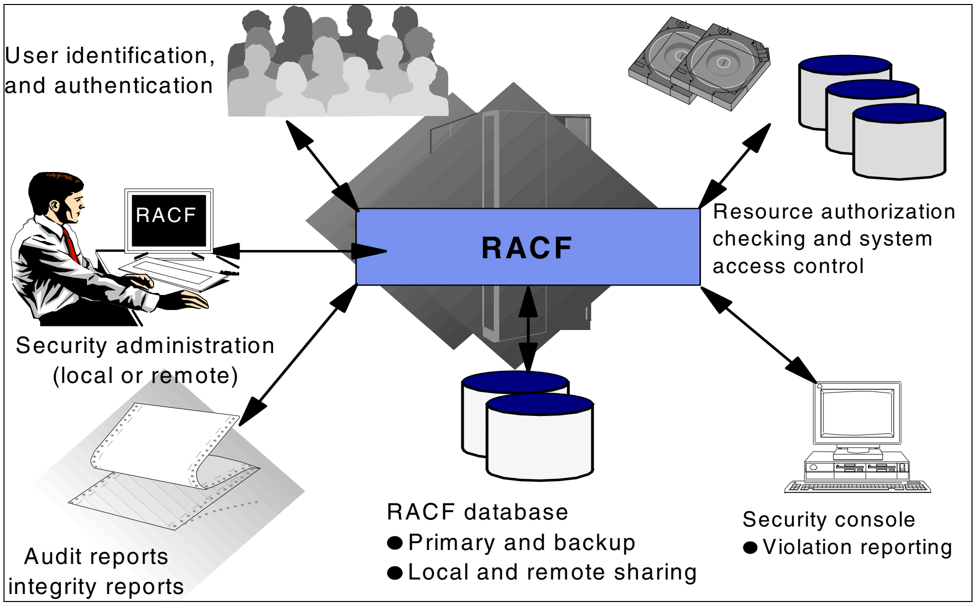


Figure 2-1 RACF overview

Digital certificates can be mapped to the RACF user ID to provide seamless access to z/OS resources, as shown in Figure 2-2.

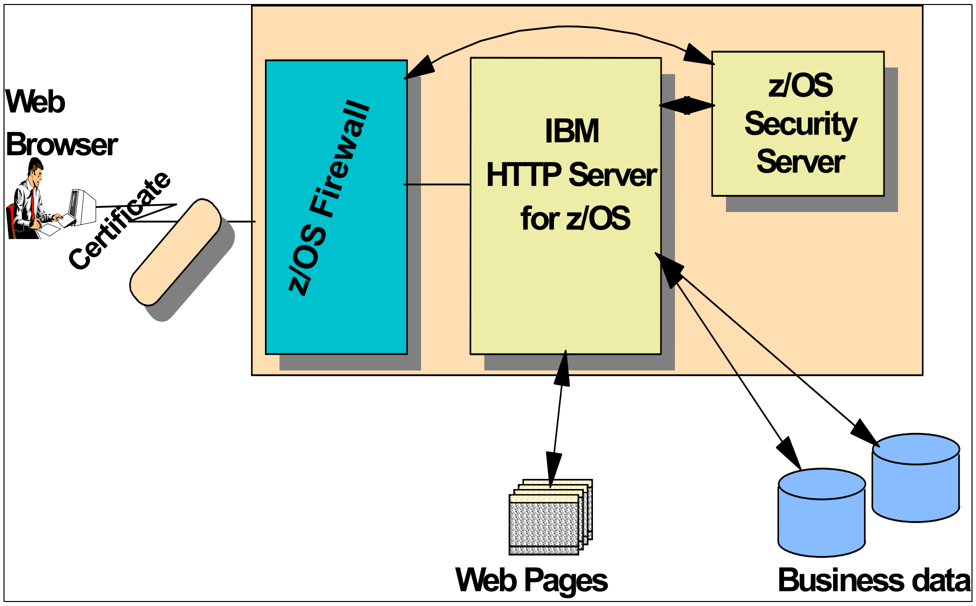


Figure 2-2 Seamless access to z/OS resources using digital certificates

Users can be enabled to self-register their digital certificates, as shown in Figure 2-3 on page 15, to ease the administration of digital certificates.

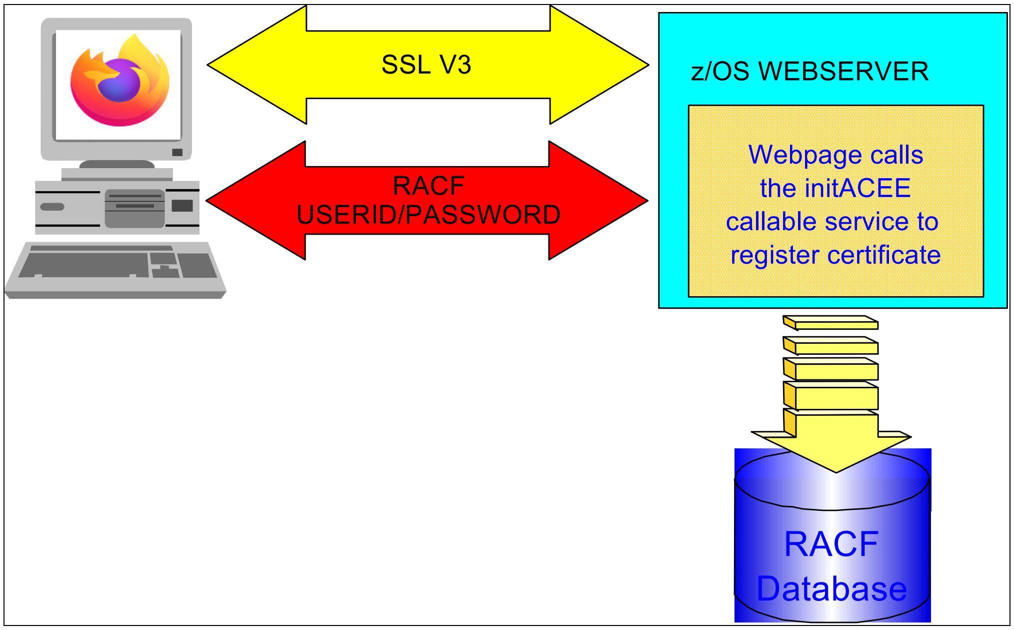

SSL V3
RACF
USERID/PASSWORD
z/OS WEBSERVER
Webpage calls the initACEE callable service to register certificate
RACF Database

Figure 2-3 Overview of the self-registration process

Certificate name filtering support was added to associate many certificates to a single, shared RACF user ID without having to install each certificate into the RACF database. Certificate filters substantially decrease the amount of database storage and the system administration requirements associated with processing large number of certificates.

With network authentication and privacy services support, it allows privacy services principal and realm information to be stored and administered in a RACF database for a Kerberos environment.

RACF program control enhancement were created to provide better security and integrity of z/OS UNIX server and daemon programs. This is accomplished by providing more control over the execution environment and preventing uncontrolled programs from entering into a controlled environment. Environment control is accomplished through a service, IRRENS00, which marks an environment as either controlled (clean) or uncontrolled (dirty).

Application identity mapping provides an improved method for associating identities defined by z/OS UNIX for z/OS.

2.1.2 The DCE Security Server

The DCE Security Server provides user and server authentication for applications using the client-server communications technology contained in the distributed computing environment for z/OS. The DCE Security Server can also interoperate with users and servers that make use of the Kerberos technology developed at the Massachusetts Institute of Technology and can provide authentication based on Kerberos tickets.

Through integration with RACF, z/OS DCE support allows RACF-authenticated z/OS users to access DCE-based resources and application servers without having to further authenticate themselves to DCE. In addition, DCE application servers can, if needed, convert a DCE-authenticated user identity into a RACF identity and then access z/OS resources on behalf of that user, with full RACF access control. Figure 2-4 shows an overview of the DCE and RACF interoperation.

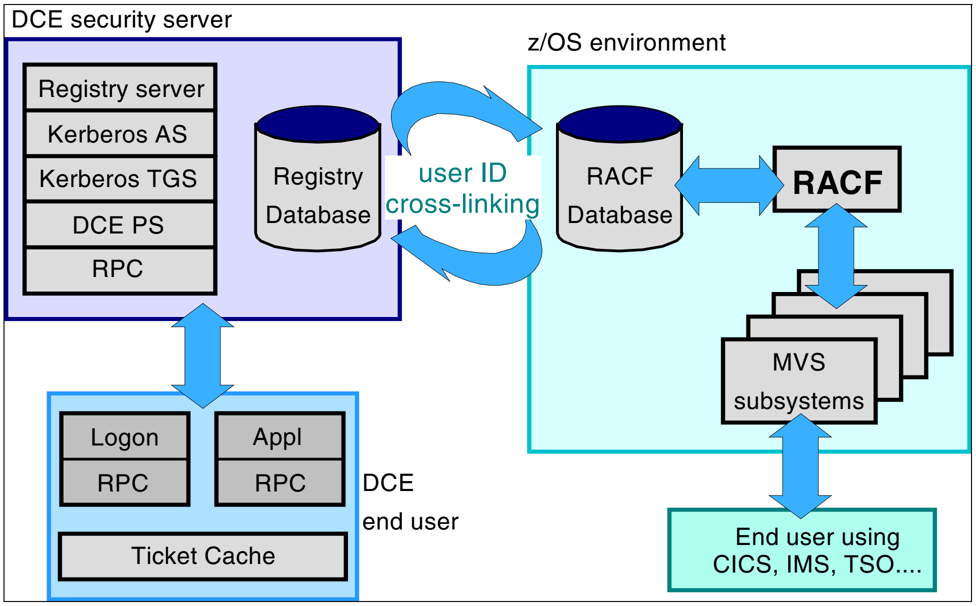


Figure 2-4 DCE-RACF interoperation

2.1.3 z/OS Firewall Technologies

Implemented partly in the z/OS Security Server and partly in the IBM z/OS Communications Server, z/OS Firewall Technologies (network security firewall program for z/OS) provide basic firewall capabilities on the z/OS platform to reduce or eliminate the need for non-z/OS platform firewalls in many customer installations.

The z/OS Communications Server provides the firewall functions of IP Packet Filtering, IP Security (VPN or tunnels), and Network Address Translation (NAT).

The z/OS Security Server provides the firewall functions of FTP proxy support, socks daemon support, logging, configuration, and administration.

z/OS Firewall Technologies has support for on-demand dynamic Virtual Private Networks (VPNs). On-demand VPNs allow an outbound Security Association (SA) to be set up automatically when the designated network traffic requires that it be transmitted securely through a VPN. Figure 2-5 on page 17 shows the potential usage of VPN technology.

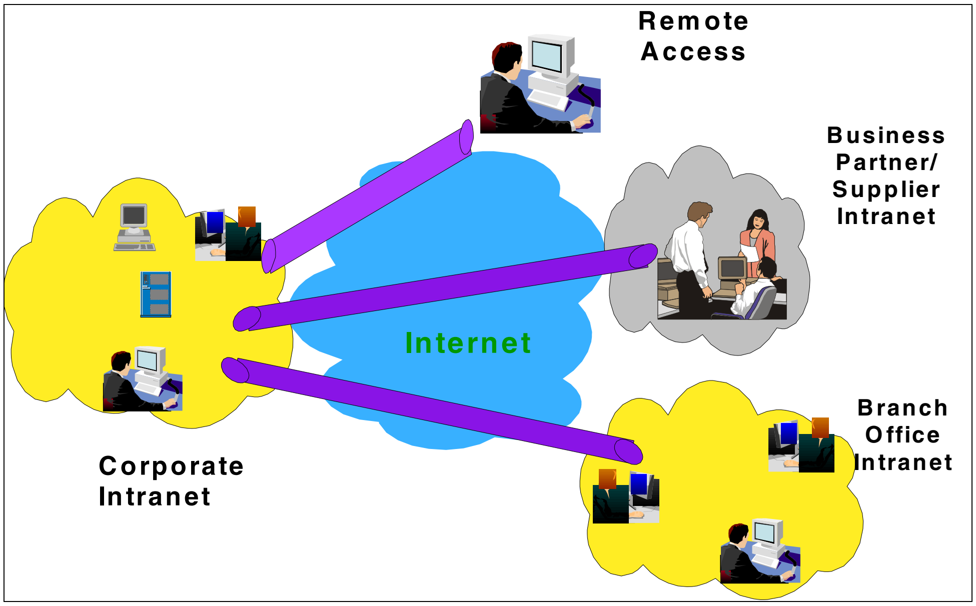
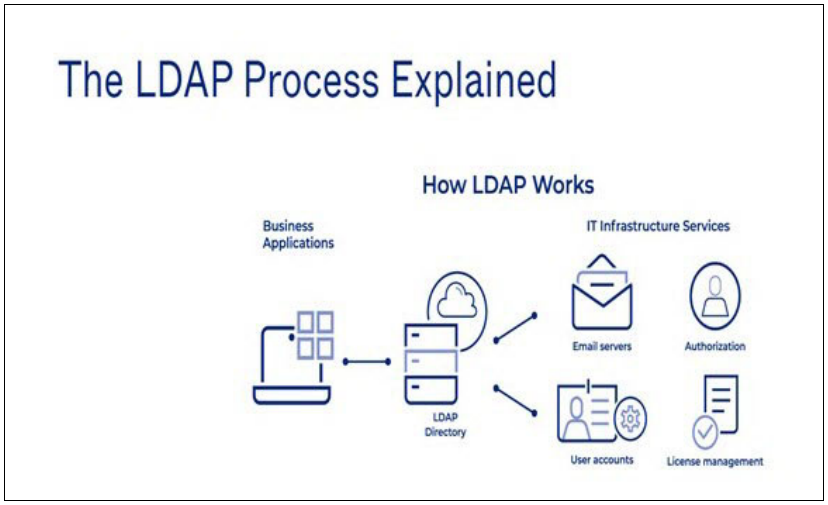


Figure 2-5 Usage of VPN technology

2.1.4 The LDAP server

The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) Network. It is used to provide a central place to store user names and passwords, allowing many different applications and services to connect to the LDAP server to validate users.


The LDAP Process Explained

How LDAP Works

Figure 2-6 LDAP process explained

RACF data presents a large set of user, group, and profile information that is useful to applications in other environments or on other systems. This item makes RACF information that is accessible through SAF interfaces available via an z/OS LDAP server to programs on and off the z/OS platform. Figure 2-7 on page 18 shows an overview of the z/OS LDAP server and the back-end systems it supports.

RACF interfaces with the z/OS LDAP server by defining proxy information about the z/OS LDAP server so that other products can communicate with an LDAP directory. It uses a proxy segment within the profile for the LDAPBIND class for communication. You can also set up a LDAP Event Notification for changes to RACF users, groups and general resources.

User ID and Password Authentication of LDAP Client Access to the z/OS LDAP Directory Server can be optionally handled by z/OS Security Server RACF rather than by accessing user IDs and passwords stored within the LDAP server directory.

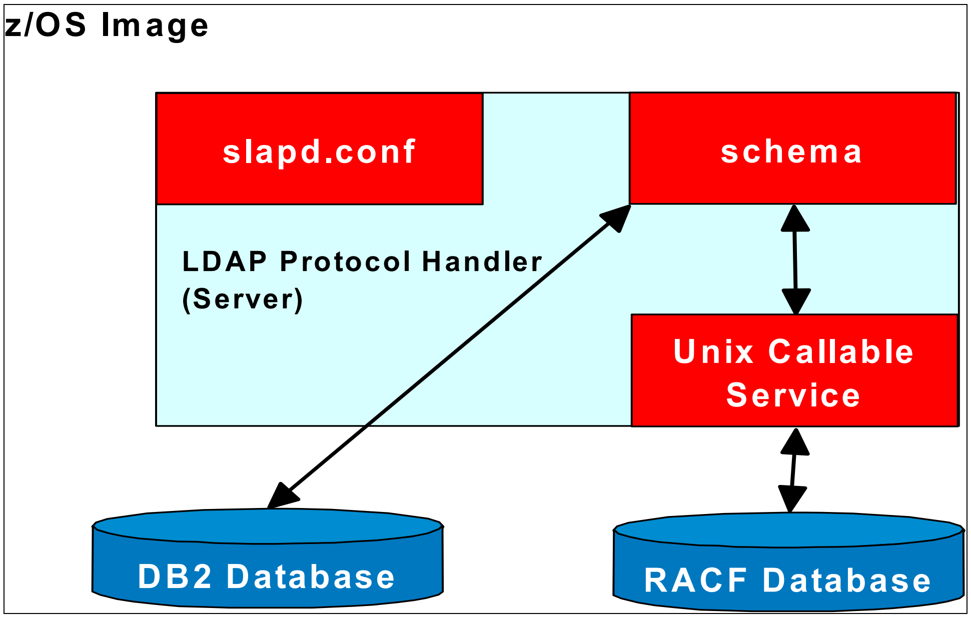


Figure 2-7 Overview of the z/OS LDAP server and supported back-end systems

2.1.5 Network authentication and privacy service (Kerberos)

Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client-server model, and it provides mutual authentication-both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

It was developed at the Massachusetts Institute of Technology in 1988 to protect network services. The Kerberos Security Technology does not require passwords to flow in readable text, because it uses encrypted tickets that contain authentication information for the users. It has been part of RACF for over 30 years going back to IBM OS/390.

Encrypted passtickets are issued by a Kerberos authentication server. Users and servers are required to have keys registered with the server and the passtickets flows to and from the servers covered by a session key. Kerberos application servers can use SAF callable services to parse Kerberos tickets to map the passtickets to RACF user(s). RACF can authenticate the user to determine if they should have access to the system.

The Network Authentication Server provides the basis of consistent user identification and authentication in a heterogeneous networked environment when combined with Kerberos-aware applications that can span z/OS and other platforms which support the Kerberos reference implementation.

The security client locates the z/OS Security Server through one of three methods:

1. By using LDAP, when the LDAP server is specified in the Kerberos configuration files.
2. By using the Domain Name Service (DNS), when DNS lookup is specified in the Kerberos configuration files.
3. By using static information contained in the Kerberos configuration files, when the LDAP or the DNS server is not available or the target realm is not defined in the directory.

Figure 2-8 shows a Kerberos implementation on z/OS.

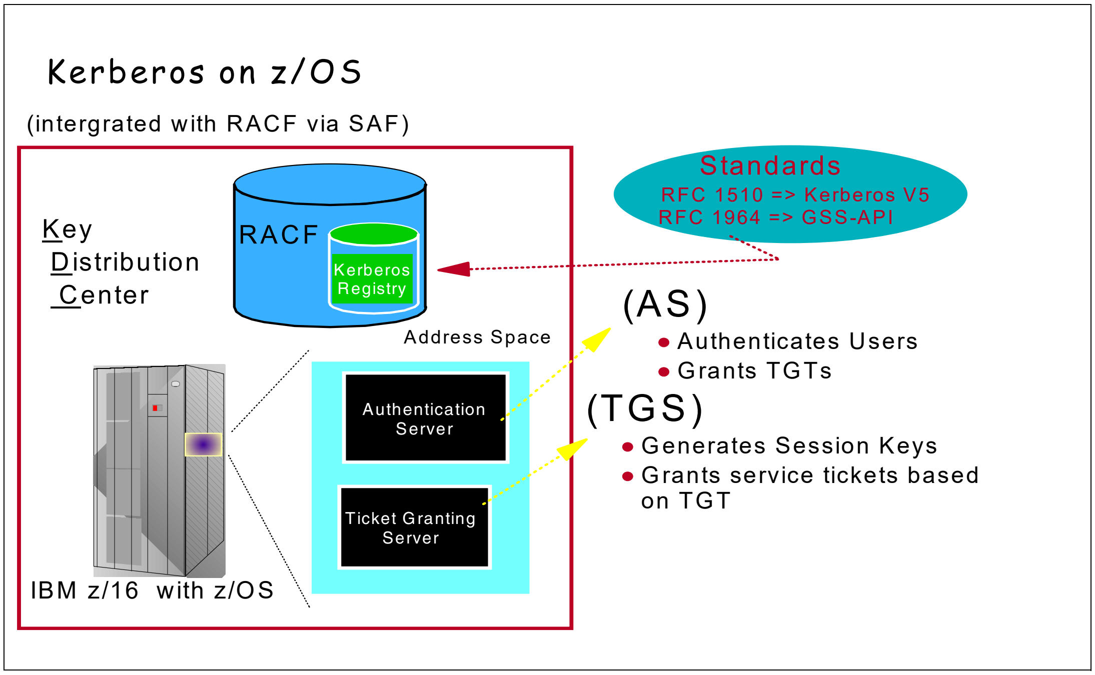


Figure 2-8 Kerberos implementation on z/OS

Figure 2-8 shows an overview of the various Kerberos pieces:

1. Kerberos registry integrated into RACF registry
2. Kerberos KDC executes within z/OS address space
3. z/OS KDC behaves like any other Kerberos “realm”
4. Kerberos realm-to-realm function supported

2.1.6 z/OS Open Cryptographic Services Facility (OCSF)

Cryptography comprehensively helps meet multiple security needs, such as confidentiality, authentication and non-repudiation. Open Cryptographic Service Facility (OCSF) for z/OS addresses these requirements in the emerging Internet, intranet, and extranet application domains. The primary application interface to this function is provided by Open Cryptographic Enhanced Plug-ins (OCEP), a component of z/OS Security Server.

OCEP functions are to be used by applications complying with Common Data Security Architecture (CDSA) standard interfaces. This makes it easier for application developers and Independent Software Vendors (ISVs) to develop and port applications to the z/OS platform. It also helps customers apply consistent security rules to applications that use digital certificates. Figure 2-9 on page 20 shows an overview of the OCSF and OCEP.

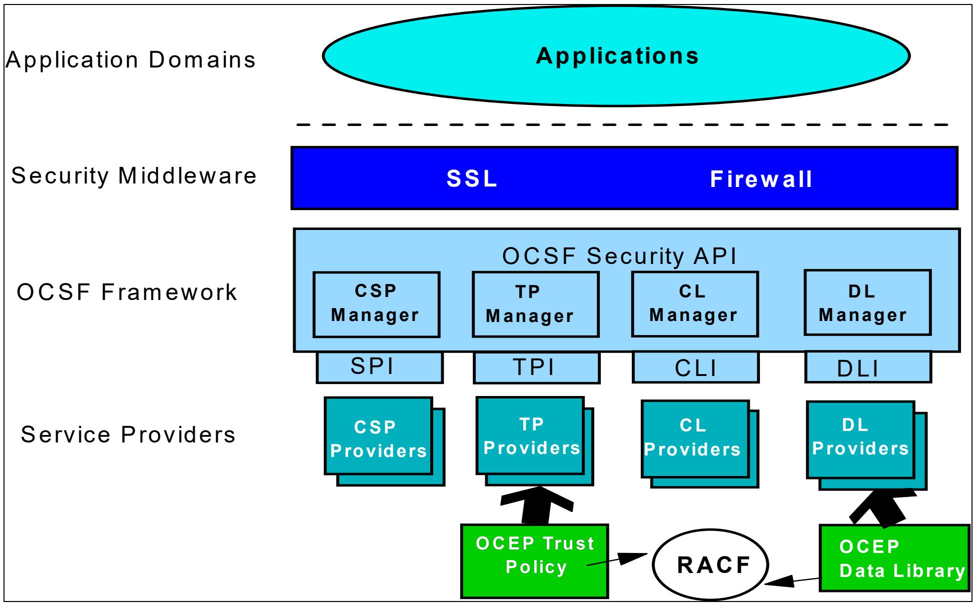


Figure 2-9 OCSF-OCEP infrastructure overview

The optional PCI Cryptographic Coprocessor (PCICC) brings additional cryptographic processing capacity and function to z/OS Parallel Enterprise Servers. The PCICC feature is intergrated into z/OS. Some people mistakenly think it is an external box.

PCICC works in conjunction with the CMOS Cryptographic Coprocessor that is standard on those servers. PCICC is not a substitute for CMOS crypto coprocessors and in fact *requires* that the CMOS crypto coprocessors be enabled. Transparently to applications, z/OS will route requests to the appropriate crypto engines for processing.

The z/OS Security Server provides “one stop shopping” for security on z/OS. With its integration of RACF and DCE Security, its contribution to the z/OS Firewall Technologies, the LDAP server, and RACF support for client authentication via digital certificates, the z/OS Security Server RACF provides complete security both for traditional host-based data processing and for safely expanding your enterprise onto the Internet.

3

IBM z/OS Security Server RACF overview

The z/OS Security Server RACF, also known as Resource Access Control Facility (RACF), is an IBM program product designed to provide z/OS and VM users with an effective tool for managing access control, an increasingly important user responsibility and concern.

The objective of RACF access control is to protect data sets and other data processing resources from unauthorized destruction, modification, or disclosure, whether by accident or design. To be effective, security procedures should be easy to use and place no additional burden upon data processing management. RACF controls users and protects resources.

Users are identified by a USER ID and authenticated by a password. A RACF user is identified by an alphanumeric user ID. However, a RACF user does not have to be an individual. For instance, a USER ID can be associated with a started task address space or a batch job.

Resources can be divided into two categories, data sets and general resources.

General resources include:

- CICS resources
- DASD
- Db2
- IMS resources
- JES resources
- NODES
- Programs
- Tape
- Terminals
- VM

There are many other resources that can be protected. For a full list of Resource Types (or Resource Classes), see *Security Server RACF System Programmer's Guide,* SA23-2287*.*

Before describing RACF resource definitions and resource access authorizations, we will explain how RACF is started and its main components. This may prove useful when we discuss conversion problems from another security product.

RACF is started during a system initial program load (IPL). There is no specific command to start RACF. So, there is no specific command to stop it.

At IPL, RACF requires the RACF primary data set names (DSN) that contain the user and resource definitions.

One way to satisfy this requirement is to place these names in PARMLIB. To activate the RACF subsystem, you must update the IEFSSNxx member of SYS1.PARMLIB, assign a RACF user ID to the RACF subsystem, review the RACF PROC in SYS1.PROCLIB. The RACF subsystem must have a valid user ID, the RACF subsystem cannot be initialized if a valid user ID is not assigned to it. The PROC name for the RACF subsystem must be the same as the name in IEFSSNxx. When using PARMLIB to supply the data set names and other options, IEASYSxx needs a line with RACF=xx. Then the member IRRPRMxx supplies the information.

Another way would be to update a DD statement (SYSRACF) in the member MSTRJCL. If MSTRJCL does not contain a proper DD statement, the final way to satisfy the requirement is that the operator is prompted for the name of the RACF database.

Points to consider for each of the three methods are:

- RACF at startup

  Requires the names of the DSN containing user and resource definitions, these names can be located in PARMLIB

- MSTRJCL

  You can define only one RACF database (the primary database). No secondary RACF database definition is allowed.

- Operator reply

  Very suitable for early tests, a conversion is an iterative process. Replying with the RACF database name at IPL time may provide flexibility to back out to a previous iteration stage if errors are encountered and the current IPL is in error.

3.1 Information and authorization flows

In this section, we describe information and automation flows.

3.1.1 Information flow

For all resources, security is processed through the system as summarized in Figure 3-1. In this process, the components involved are listed in the leftmost part of the figure. They are (top to bottom):

- A subsystem (such as JES) or an application
- The System Authorization Facility (SAF), which is part of z/OS
- RACF
- The RACF database

The role of each component in the security process is discussed in later topics. The information that is passed is discussed in the following sections.

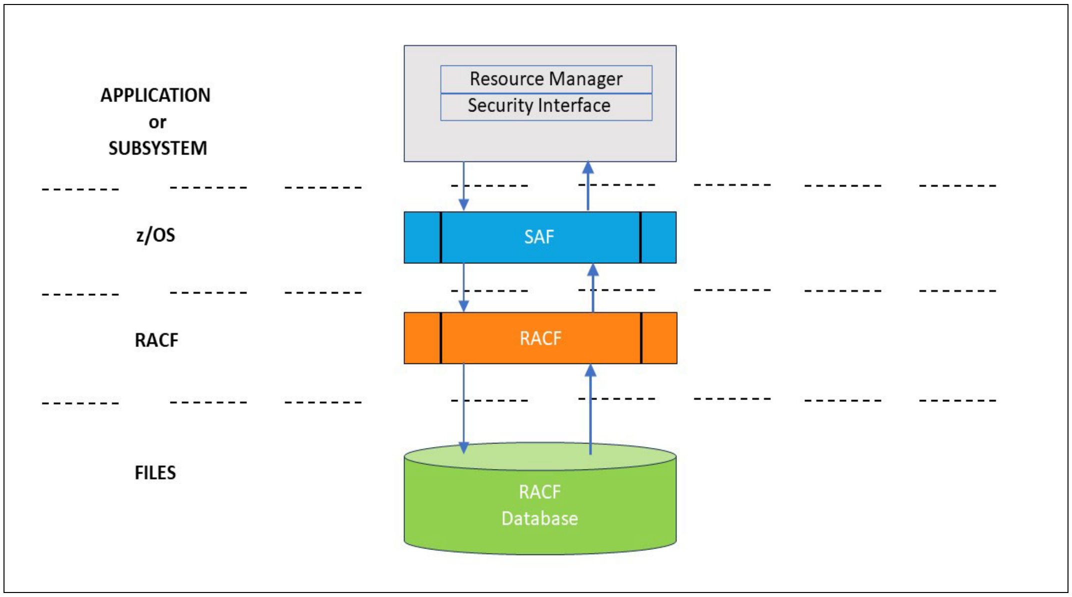


Figure 3-1 Information flow for RACF

The application directs a request to RACF. Depending on the type of request, information is passed along with the request, as shown in the following two examples.

Example 1

```
Request to RACF : Verify user identity
Information passed    : USERID and PASSWORD
```

Example 2

```
Request to RACF       : Check user access to a resource
Information passed    : USERID
                        Resource name and type
                        User intent
```

The security interface formats the information gathered by the application to be used by the security monitor (here RACF) and passes it to the System Authorization Facility (SAF).

SAF determines what actions are required to process the request and may forward the request to RACF if needed. If requested, RACF then performs the check by verification against data retrieved from the RACF Database. Although Figure 1 may indicate an input operation is performed, RACF data is often retrieved from areas in storage and no input operation takes place.

RACF always returns a return code as a response to a request. A reason code may also be returned. For list-type requests, RACF also returns the requested data.

A return code of zero (0) indicates a valid request. A non-zero return code of four (4) may be acceptable, depending on the resource manger giving the message, a return code of eight (8) indicates an error. These return codes are passed to the resource manager that issued the request. It is up to the resource manager to take appropriate action.

The logical functions of each component are as follows:

- Interface Role
  - Receive and format information from the application.
  - Route information to the SAF facility.
  - Receive a return code from RACF and return it to the caller.
- SAF Role
  - Route the request to the security monitor.
  - Route the response to the proper requestor.
- RACF Role
  - Send back a return code and reason code as a response to a security request.
  - Add, modify, or delete profiles in the database as required by RACF commands executed by an authorized user.
  - Set global option values as directed by authorized users.
  - Return requested information from the database in response to a list-type command.

3.1.2 Authorization Flow

For all resources, security authorization is processed through the system as summarized in Figure 3-2. For more information on authorization flow, see *z/OS Security Server (RACF) Security Administrator's Guide, SA23-2289*.

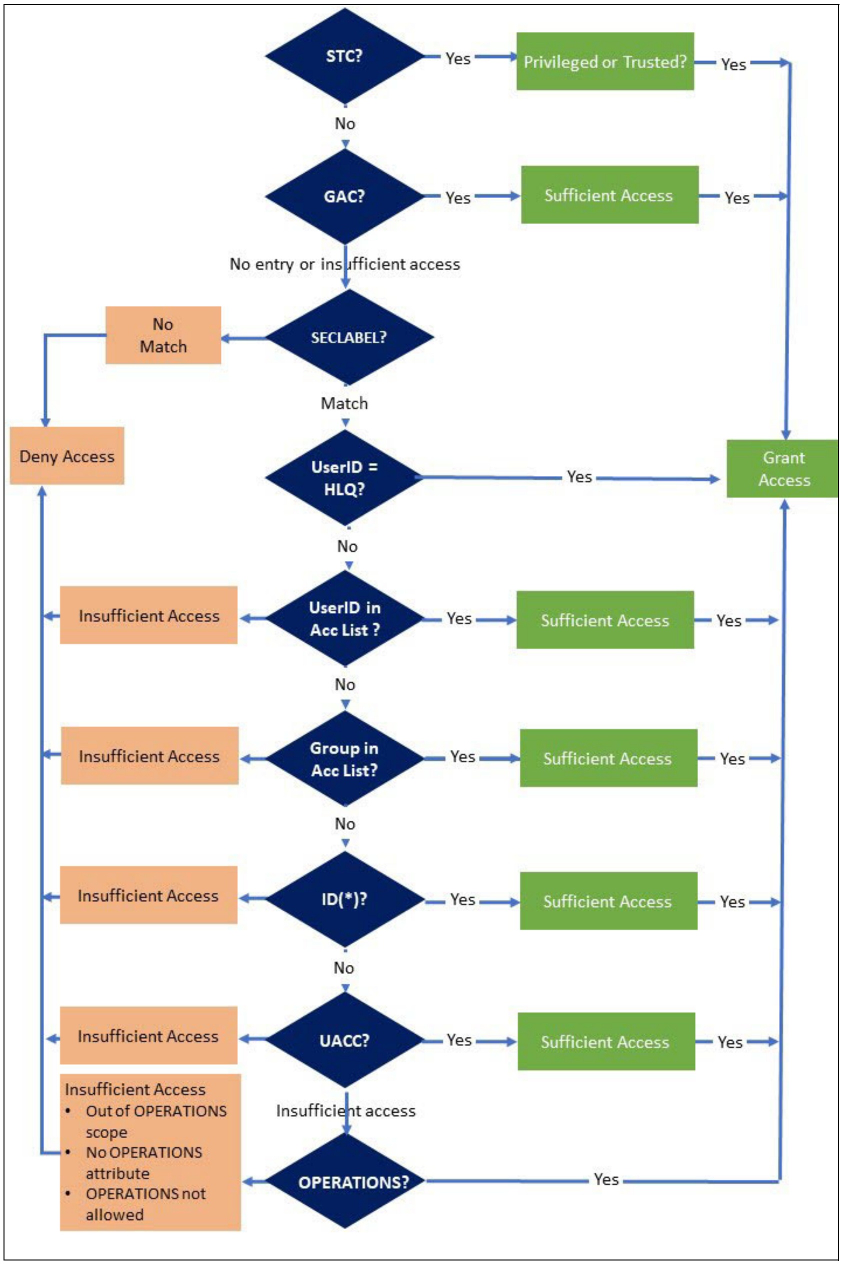


Figure 3-2 Authorization flow for RACF

3.2 Vocabulary

This section defines terms used in RACF.

3.2.1 RACF USER

A RACF user is always defined as a member of a RACF group. This group is called its *default group*. An entry in the RACF database describing a user is called a *user profile*.

A user profile describes the user by name (user ID), password, default group, the times that user can use the computing system, and statistics on a prior logon by the user. It also describes other groups the user may belong to. A user must be a member of at least one group (the default group), and potentially of other groups (connect groups).

User profiles may also contain *user attributes*. These attributes describe the privileges and restrictions that the user has when using the system. Attributes are classified as either user-level or group-level attributes. When attributes are assigned at the user level, the scope of the attributes are at the system level and privileges granted are across the entire system. When attributes are assigned at the group level, the corresponding privileges are restricted to a group or the scope of the group in which attributes are assigned. Related product data may also be recorded in user profiles. The set of data for a specific product is called a segment. At the user level, there may be segments for

- DFP
- LANGUAGE
- NDS
- NETVIEW
- OMVS
- OPERPARMS (for MCS extended console sessions)
- OVM
- TSO
- WORKATTR (for APPC/z/OS processing)

For more information on each Segment's content, see the corresponding topic in this book, or in *z/OS Security Server (RACF) Command Language Reference* SA23-2292.

The ability to define attributes at the System or Group Level is used to build the correct administrative structure for RACF. The **SPECIAL** and **AUDITOR** attributes, defined at the appropriate level, are used to achieve centralized or decentralized security administration.

For conversion purposes, users are often classified as:

- TSO users
- STC (or started task users)
- Others

In the RACF database, there is no special definition for a TSO user, an STC user, or other users. All are RACF users. The Default Group, Attributes, and other values in the Profiles make the difference. It should be noted that a RACF user ID can range from one to eight characters in length, but a RACF user ID used for TSO LOGON must not be longer than seven characters.

3.2.2 RACF group

A RACF group consists of all the users that have similar requirements for access to the system's resources. Each group, with the exception of the highest group (SYS1), has a superior group. A RACF group is identified by its name. The name of a group is one to eight alphameric characters, the first being alphabetic or special characters.

An entry in the RACF database describing a group is called a group profile. A group profile contains the group name, the superior group, the owner name (if not the superior group), a list of all RACF groups that have the described group as its superior group, and a list of user IDs that are members of the group.

The *scope* of a group is confined to all resources and users within that group and those of all groups that are subordinate to that group.

Related product data may also be recorded in group profiles. The set of data for a specific product is called a *segment*. At the group level, there may be segments for:

- DFP
- OMVS
- OVM
- TME

3.2.3 Owner

Each entry (or profile) in the RACF database has an *owner*. The owner must be a RACF-defined USER or GROUP. For ease of administration, group ownership is preferred. The RACF owner of a profile has full administrative authority over the profile. If the profile is a user or a group profile that is in turn designated as the owner of other profiles, the RACF owner of the top profile has full administrative authority over the other profiles.

3.2.4 RACF protected resources

RACF resources are all the components of a computing complex required by a job or a task. RACF resources include input/output devices, processing units, data sets, job output, nodes, programs, and other items that must be kept secure for normal business operations.

RACF protected resources can be divided into two categories:

- Data sets profiles
- General resources profiles

Both are considered *resource profiles*. RACF subdivides resource profiles into two types: discrete profiles and generic profiles.

A *discrete profile* protects a single resource that has unique requirements. This profile contains a description of the resource, including the authorized users, the access authority of each user, and in the case of data sets, the volume of the data set.

A *generic profile* protects several resources that have a similar naming structure and security requirements. This profile contains a description of the resources, including the authorized users and the access authority of each user. For more information on discrete and generic profiles, see *z/OS Security Server (RACF) Security Administrator's Guide SA23-2289*.

Data sets

Data set resources include both DASD and TAPE data sets, and are described in the RACF database as *data set profiles*. A data set profile contains information about the data set profile owner, universal access, and other optional information, such as the device volume serial number and data set security classification.

Before a data set profile can be created in the RACF database, a group profile or user profile having the data set high-level qualifier (HLQ) as the group or user name must be defined.

This group or user is used in the RACF database as an anchor point for all profiles having the same HLQ.

Therefore, protection for a data set always includes at least two entries (but optionally more) in the RACF database

- A group profile or user profile (with same name as the data set HLQ)
- One or more data set profiles (either discrete or generic)

When a data set can be protected by several different profiles, RACF searches for the best-fitting profile. The search is made from the most specific profile to the least specific. Access is then granted or denied according to the security classification associated with the data set and the user requesting access, the access lists contained in the selected resource profile, and user attributes.

General resources

A *general resource* is any resource other than a data set. For example, transactions, TSO logon procedures and job SYSOUT are general resources. RACF defines the set of general resources in a Class Descriptor Table (CDT), which identifies a RACF class of entities by the resource class name. This table includes the resource class name, all syntax rules, and auditing and statistical control.

A standard IBM-supplied CDT is installed with RACF at initialization time. You can append your unique class names to the standard CDT to represent your installation's requirements outside of those identified by RACF. For more information on the Class Descriptor Table and on how to add new resource classes, see *Chapter 10. Administering the dynamic class descriptor table (CDT)* in the *z/OS Security Server RACF Security Administrator's Guide.*

A conversion to RACF may require you to add installation-defined classes to the standard CDT.

Protection of a general resource can be achieved through use of one or several profiles, either specific or generic. Note that:

- No anchor point is needed for general resource profiles (unlike data-set profiles).
- Authorization is the same as for data sets.

For most of the general resource classes, a relationship exists between a class called a *member* class and another class called a *grouping* class.

The class TCICSTRN, for example, is a standard RACF resource class in which one can create profiles to protect one or several similarly named CICS transactions.

For example:

- A transaction named TRN1 can have a profile in the TCICTRN class with a resource name of TRN1.
- All transactions whose names begin with TRN can have a profile in the TCICSTRN class with a resource name of TRN*.

But we may wish to define transactions TRN5, TRTA, and XYZ as having the same protection and authorization requirements.

We can then use the CICS grouping resource class name of GCICSTRN. Our grouping transaction profile can then be defined in the GCICSTRN class with a name of MYOWNAME and members TRN5, TRTA, and XYZ. This profile will then control access to all the member transactions. MYOWNAME is an arbitrary unique name within the

GCICSTRN class. This name is assigned by the installation to be a meaningful mnemonic. Grouping classes should be considered when converting protection rules from another security system.

3.2.5 RACF system-wide options

RACF system-wide options are used to customize RACF for installation-specific security. Mainly, these options deal with:

- Auditing
- Statistics
- Activation of classes
- Use of generics
- In-storage profiles
- JES job verification
- Default JES user IDs
- Data set protection and access
- Password rules
- SECLABELS
- Default language

Setting appropriate values for all general options in order to provide equivalent RACF functions when converting from another security product is part of the conversion project. When needed, changes to these values are mentioned in the appropriate chapters. For a complete description of RACF options, see *z/OS Security Server (RACF) Command Language Reference* SA23-2292 and *z/OS Security Server (RACF) Security Administrator's Guide SA23-22*89.

3.2.6 The RACF database

There is only one RACF database, which holds the following:

- System options
- User profiles
- Group profiles
- Data set profiles
- General resource profiles

For performance purposes, this one database can be broken into several files spread across system DASD volumes.

For recovery purposes, this base can be mirrored onto another database. The main database is referred to as the *primary database*. The mirror database is referred to as the *secondary database*.

Modifications to the primary database are reflected in the secondary database at the time they occur. RACF database definitions allow flexibility in the information to be mirrored, providing the secondary database is online and active.

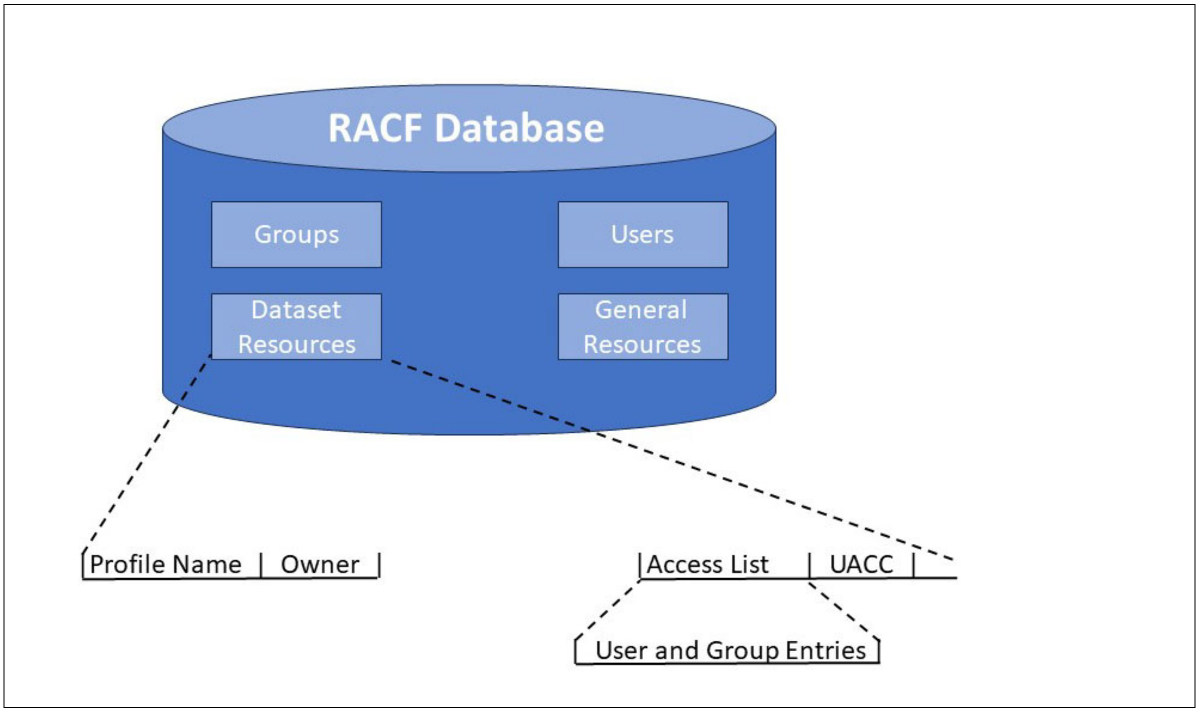


Figure 3-3 Database structure for RACF

3.2.7 RACF commands

RACF commands are TSO/E commands that may be executed either online from a TSO terminal or as a part of a batch TMP job. RACF panels and REXX procedures are both available in addition to the online commands.

In following chapters we will see that one of the main tasks in a conversion process is the generation of many RACF commands. These typically will be used as input to several batch TMP jobs to load the RACF database with security information. Creation, review, edit, and execution of such files is an iterative process during the conversion. The following is a brief review of the main commands:

- Commands directed to USER Profiles:

ADDUSER (AU)	Add User Profile
ALTUSER (ALU)	Alter User Profile
DELUSER (DU)	Delete User Profile
DELUSER (DU)	Delete User Profile
LISTUSER (LU)	List User Profile
PASSWORD (PW)	)Specify User Password
CONNECT (CO)	Connect User to Group
REMOVE (RE)	Remove User from Group
SEARCH (SR)	Search for User Profiles

- Commands directed to Group Profiles:

ADDGROUP (AG)	Add Group Profile
ALTGROUP (ALG)	Alter Group Profile

DELGROUP (DG)	Delete Group Profile
LISTGRP (LG)	List Group Profile
SEARCH (SR)	Search for Group Profiles

- Commands directed to Data-Set Profiles:

ADDSD (AD)	Add Data Set Profile
ALTDSD (ALD)	Alter Data Set Profile
DELDSD (DD)	Delete Data Set Profile
LISTDSD (LD)	List Data Set Profile
PERMIT (PE)	Maintain Data Set Access List
SEARCH (SR)	Search for Data Set Profiles

- Commands directed to General-Resource Profiles:

RDEFINE (RDEF)	Define General Resource Profile
RALTER (RALT)	Alter General Resource Profile
RDELETE (RDEL)	Delete General Resource Profile
RLIST (RL)	List General Resource Profile
PERMIT (PE)	Maintain General Resource Access List
SEARCH (SR)	Search for General Resource Profiles

- Others (RRSF, System, etc.):

DISPLAY	Display Sign-On-From List
HELP (H)	Obtain RACF Help
RACDCERT	RACF Digital Certificate
RACLINK	Administer User ID Associations
RESTART	Restart RRSF Functions
RVARY	Change status of RACF database
SET	Set RRSF Operational Characteristics
SETROPTS (SETR)	Set RACF Options
SIGNOFF	Sign Off Session
STOP	Shutdown RRSF
TARGET	Define RRSF Nodes

Figure 3-4 shows an overview of all RACF commands.

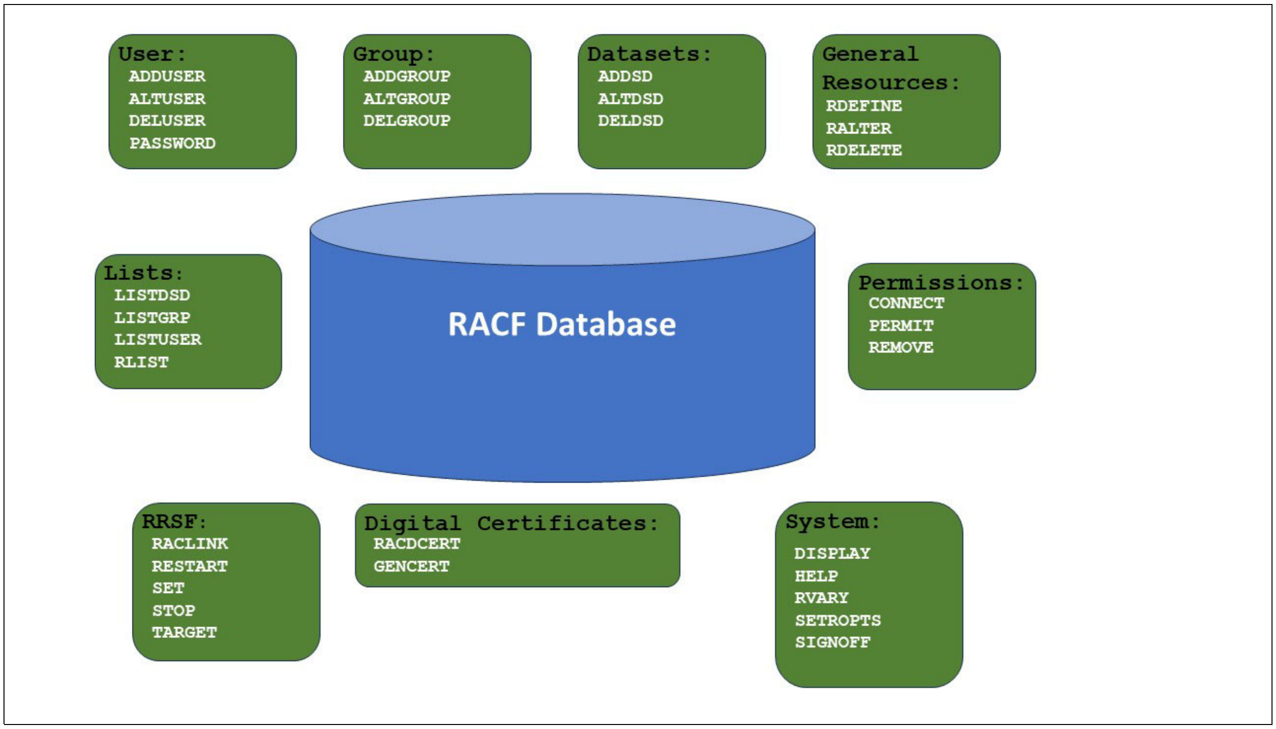


Figure 3-4 Commands for RACF

Complete details about each command can be found in *z/OS RACF Command Language Reference,* SA23-2292.

3.3 Interfaces

This section describes the interfaces to RACF.

3.3.1 Product Interfaces

Products may or may not have security Interfaces to RACF. RACF product or application interfaces fall into three categories:

- Implicit

  A product interface to RACF is *implicit* when no parameter value settings are needed in the product to enable it to use RACF for security controls. For example, products such as JES2 or TSO/E have implicit interfaces.

- Explicit

  A product interface to RACF is *explicit* when parameter value settings are needed in the product to enable it to use RACF for security controls. For example, products such as CICS and IMS have Explicit Interfaces.

- Exit Driven

  If neither an implicit nor an explicit interface to RACF exists for a product, the installation can create the interface by using standard API. The security requests are called from standard product exits. This approach can also be used to create interfaces to RACF from within applications.

One of the major problems in converting from another security system to a RACF security system is the inventory of all interfaces used by the non-RACF security product. We may discover that an exit interface has been used by the non-RACF security product in order to bypass a standard implicit interface to RACF, or parameter values to activate RACF from an explicit interface have not been set.

Re-establishing use of standard interfaces is one part of the conversion task.

3.3.2 The SAF interface

The System Authorization Facility (SAF) is a part of z/OS and is always active. Any security product can use the SAF Interface. The main purpose of SAF is to route requests from applications or subsystems to the proper security component for processing. This routing uses the SAF Router Table. Depending on the type of request SAF may, or may not, invoke RACF Services.

For a description of SAF and how to add entries in the SAF Router Table, see *z/OS Security Server RACF System Programmer's Guide,* SA23-2287.

3.3.3 RACF exits

RACF provides exit points that can be used for additional levels of protection. Figure 3-5 shows all the exits that RACF currently supports. Most installations will not need to code these exits. Where possible, standard RACF functions should be used.

The following section gives a brief description of some of the more common exits and their possible uses. You can verify which exits are active by reviewing the RACF DSMON report. Some exits can do both pre- and post-processing. Normal RACF usage does not require the use of any exits. The exits provide interfaces for changing normal RACF processing.

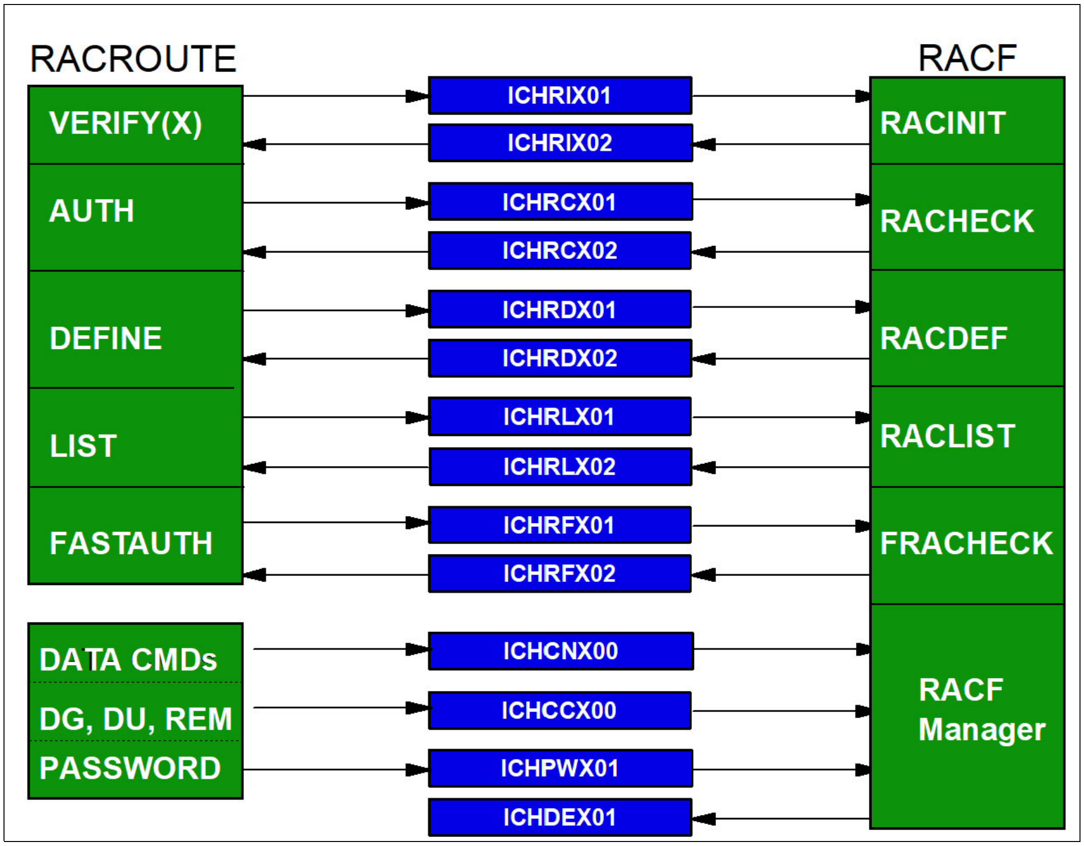


Figure 3-5 RACF exits

- Command exits - ICHCNX00/ICHCCX00

  These exit routines allow the installation to associate additional security checking, or processing, with certain RACF commands, or to bypass checking altogether.

- Authorization exits - ICHRCX01/ICHRCX02

  The **RACROUTE REQUEST=AUTH** exits can alter the decision-making process that determines if a user should have access to a resource.

- Define exits - ICHRDX01/ICHRDX02

  The **RACROUTE REQUEST=DEFINE** exits can alter the creation (or deletion) of profiles. These might be used to enforce local standards.

- Verify exits - ICHRIX01/ICHRIX02

  The **RACROUTE REQUEST=VERIFY(X)** exits can alter the authentication processing for a user.

- Password encryption - ICHDEX01

  This exit can be used to alter the form in which passwords are stored.

- Password checking exit - ICHPWX01

  This exit can be used to check for trivial passwords and enforce local password rules in addition to normal RACF password rules.

- Data set naming convention table - ICHNCV00

  This table allows the installation to set up and enforce data set naming conventions that are different from standard RACF naming conventions. For example, you may need to perform RACF checking on the second-level qualifier of a data set and not the first, which is the way RACF normally works.

4

Broadcom Top Secret overview

This chapter briefly describes the Broadcom Top Secret security product.

4.1 The Broadcom Top Secret philosophy

The way Broadcom Top Secret protects data sets (and all other resources) is sometimes referred to as “protection based on the user”. This means that, when deciding whether a user can access a certain data set, Broadcom Top Secret starts with the users Accessor ID (ACID), and then checks for the appropriate XA DATASET rules that are assigned specifically to that user.

By default, all resources (any component of the operating system required by a task) are *not* protected on a system with Broadcom Top Secret installed and active. You must set system-wide or resource-specific options to enable access to resources. The four modes of operation in Broadcom’s Top Secret are:

- DORMANT - Broadcom Top Secret is installed and is *not* actively validating resources.
- WARN - Broadcom Top Secret is active, and validating resources, but instead of failing requests, it generates warning messages.
- IMPL - Broadcom Top Secret is active, validating resources, and failing unauthorized access requests. Undefined users can operate normally, but are restricted from defined resources.
- FAIL - Broadcom Top Secret is in full control of resources.

For example, for data sets, RACF has the **PROTECTALL** option with values of **FAILURES** and **WARNING**. These values help map the Broadcom Top Secret **MODE** Parameter values (**FAIL** and **WARN**).

In Broadcom Top Secret, the data sets a user can access are determined by checking the XA DATASET rules related to that user. These rules are found in both the individual user ACID and any profile ACIDs the user belongs to.

There are three checking sequences, depending on which Broadcom Top Secret startup option is used. If **AUTH(OVERRIDE,ALLOVER)** is used (the more common one), then the checking sequence is:

1. Rules in the user ACID are checked. If a rule meets the criteria, no further checking is performed.
2. Rules in any profiles assigned to the user are checked, and each profile is checked in the order that it is listed in the user ACID. If a rule meets the criteria, no further checking is performed. If multiple accesses for a resource are located, access is granted or denied based on the access rule containing the most specific match.
3. Rules in the ALL record are checked.

Another checking sequence used by Broadcom Top Secret is **AUTH(OVERRIDE,MERGE)**. It merges all of the rules in the user profile and all profiles connected to the user, and then chooses the most appropriate one. An access decision is not made until the entire merged record is searched. If no match is found, the **ALL** record is searched. If a rule meets the criteria, no further checking is performed. If multiple accesses for a resource are located, access is granted or denied based on the access rule containing the most specific match.

Figure 4-1 shows these sequences.

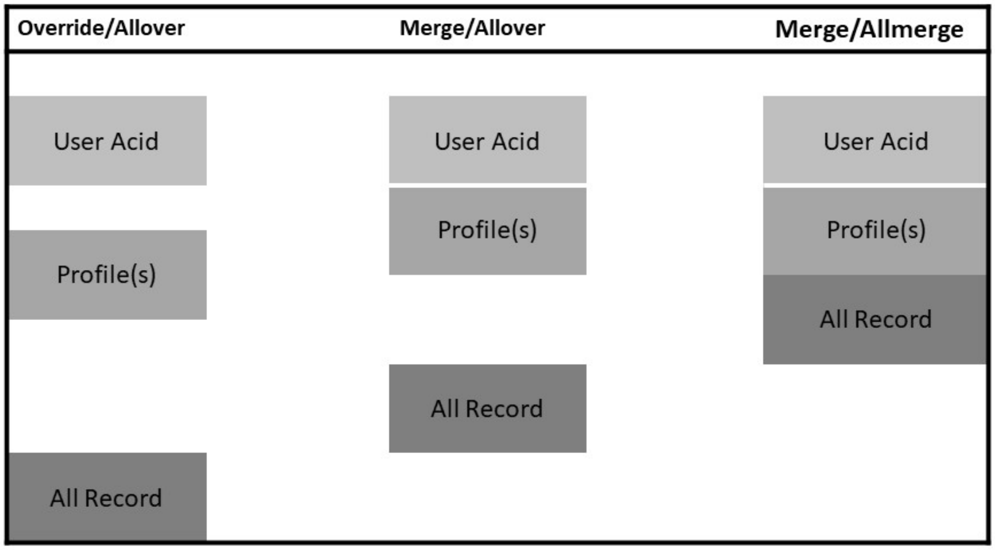


Figure 4-1 Broadcom Top Secret access checking sequences

The following example shows a user's access to a resource in each of the **AUTH** options:

- User ACID = USER01
- Profiles = PROF01 and PROF02, and they are assigned to USER01 in that order
  - USER01 contains the following resource definitions:
    - XA DATASET - TECH.TEST.APPS01 - ACCESS = READ
    - XA DATASET - TECH.*.APPS01.LOADLIB - ACCESS = UPDATE
  - *PROF01* contains the following resource definition:
    - XA DATASET - TECH.TEST - ACCESS = UPDATE
  - *PROF02* contains the following resource definition:
    - XA DATASET - TECH.*.APPS01.LOADLIB - ACCESS = NONE
- The ALL Record contains the following resource definition:
  - XA DATASET - TECH.TEST.APPS01.LOADLIB - ACCESS = EXECUTE

USER01 access level to data set **TECH.TEST.APPS01.LOADLIB** in each of the three different **AUTH** options would be determined from the following XA data set rules:

- Override/Allover:
  - XA DATASET- TECH.*.APPS01.LOADLIB - ACCESS = UPDATE
  - Reason - it was in the user's profile and had the most number of characters.
- Merge/Allover:
  - XA DATASET - TECH.*.APPS01.LOADLIB - ACCESS = NONE
  - Reason - it was one of the two rules that had the most number of characters and it had an access level of NONE.
- Merge/Allmerge:
  - XA DATASET - TECH.TEST.APPS01.LOADLIB - ACCESS = EXECUTE
  - Reason - the **ALL** record is included in the merge and it had the most number of characters.

The RACF security philosophy

The way RACF protects data sets (and all other resources) is sometimes referred to as “protection based on the resource”. This means that, when deciding whether a user can access a certain data set, RACF starts with the data set profile, and then checks the access list of that profile for an appropriate *USER* or *GROUP*.

ACIDs fall into one of two categories:

1. Functional ACIDs used to perform specific tasks:
   - User - This is the lowest level of ACID security in Broadcom Top Secret and is used to define a person who can log onto a system. User ACIDs are converted to RACF users.
   - Profile - This is an ACID containing a collection of access characteristics. This ACID cannot sign on. Profile ACIDs are converted to a RACF group that is owned by the equivalent of a Broadcom Top Secret division or department.
   - Group - This ACID contains a collection of users who can share access authorities for protected resources.
   - Control - This ACID is used to define security administrators.
2. Organizational ACIDs used to construct the security database hierarchy:
   - Department - This is an ACID definition in Broadcom Top Secret describing where a user usually works. Each user ACID needs to be associated with a department. Department ACIDs are converted to a RACF group that is owned by the equivalent of a Broadcom Top Secret division.
   - Division - This is an ACID used to define corporate hierarchy in a company’s corporate security structure. Division ACIDs are converted to a RACF group.
   - Zone - This is an ACID used to group two or more divisions.

Broadcom Top Secret profiles become what the *z/OS Security Server (RACF) Security Administrator’s Guide,* SA23-2289 refers to as “functional groups”. Both products use this concept in the same way. Typically, all resources needed to perform a particular function are permitted to the same Broadcom Top Secret profile (or RACF functional group), rather than to each individual user performing that function. Each product has a way of associating the right users with the right Broadcom Top Secret profiles or RACF functional groups.

In RACF, functional groups usually do not “own” any users; that is, no users have these groups as their default group. Users instead are connected to these groups in order to access the resources that these functional groups are permitted to use.

The term profile has a different meaning in RACF than the Broadcom Top Secret definition given above. Refer to the *z/OS Security Server (RACF) Security Administrator’s Guide, SA23-2289* for the precise definition of the term as used by RACF.

Broadcom Top Secret is started as a task by the `START` command, and executes in its own address space. Broadcom Top Secret execution is stopped by entering a `STOP (P)` command (with the proper procedure name) on a z/OS operator console.

All Broadcom Top Secret data is stored in the Broadcom Top Secret security file in an encrypted format.

4.2 The Broadcom Top Secret environment

The following sections describe the Broadcom Top Secret environment and staffing.

4.2.1 The ALL record

There are times in Broadcom Top Secret when a user tries to access a data set, and there is no appropriate XA DATASET rule in either the user ACID or any of the profile ACIDs. For those situations, the **ALL** Record is used by Broadcom Top Secret (when the **OVERRIDE,ALLOVER** option in Broadcom Top Secret is in effect).

This record is a list of resource rules (data set and others) similar to a profile, except it is always the last place Broadcom Top Secret looks for a resource rule to check against. If an appropriate rule cannot be found in the **ALL** record, then access to the resource depends on the overall security mode that Broadcom Top Secret is in (**WARN, IMPLEMENT,** and so on).

The functions of the **ALL** Record in Broadcom Top Secret are handled by the *UACC* (Universal Access Authority) in RACF. The **UACCs** are not stored in one central RACF list, but are defined separately for each RACF profile.

4.2.2 Personnel

Broadcom Top Secret administrators are needed to obtain information on how Broadcom Top Secret is implemented in the installation. The following describes the personnel involved in the security administration in Broadcom Top Secret.

The Broadcom Top Secret administrative hierarchy

The Broadcom Top Secret administrative hierarchy has the following levels:

- Master Security Control ACID (MSCA) is converted to RACF System-Special.
- Central Security Control ACID (SCA) is converted to RACF System-Special.
- Limit Central Security Control ACID (LSCA) is converted to RACF Group-Special.
- Zone Control ACID (ZCA) is converted to RACF Group-Special.
- Divisional Control ACID (VCA) is converted to RACF Group-Special.
- Departmental Control ACID (DCA)- is converted to RACF Group-Special.

Broadcom Top Secret officer

The security officer with the MSCA or SCA attribute will be able to give you most of the information you need to convert the Broadcom Top Secret database into RACF commands.

Broadcom Top Secret auditor

The security auditor has the same duties in both the Broadcom Top Secret and RACF environments. The Broadcom Top Secret auditor can give you information on Broadcom Top Secret database contents, and on the reporting and auditing level needed.

z/OS systems programmers

These programmers will be responsible for all z/OS/JES/TSO Exits and user modifications. They are needed for maintaining libraries, modules, procedures, and parameters.

Product systems programmers

These programmers will be responsible for converting and updating all product interfaces to RACF.

Broadcom Top Secret has control options to define the security environment. These options are defined in the Broadcom Top Secret parameter File. Some examples include Password Definition, Mode, Tape Dataset Security, Facility, and Violation Logging.

4.2.3 Resource rules

Securing resources in Broadcom Top Secret is a two-step process.

1. Once the resource has been defined, it needs to be owned by an Individual user ACID or a department ACID.
2. Once the resource has been owned, it can then be permitted to additional users if needed.

In Broadcom Top Secret, a resource protection definition is called a resource rule. Some examples of resource rules are:

- XA Dataset for Dataset Protection
- XA Facility for Application Protection
- XA Terminal for Terminal Protection
- XA Otran for Transaction Protection

Broadcom Top Secret access authority is defined as follows:

- ALL - converts to RACF equivalent of ALTER
- SCRATCH converts to the RACF equivalent of ALTER.
- CREATE converts to the RACF equivalent of ALTER.
- CONTROL converts to the RACF equivalent of CONTROL.
- WRITE converts to the RACF equivalent of UPDATE.
- UPDATE converts to the RACF equivalent of UPDATE.
- READ converts to the RACF equivalent of READ.
- FETCH converts to the RACF equivalent of EXECUTE.

Some XA DATASET rules also have a FACILITY subparameter. A FACILITY is a way of grouping options and associating them with a particular service that users sign on to. Some facilities supported are CICS, TSO, BATCH, and STC. In Broadcom Top Secret, you can restrict access to a data set to certain applications by using the FACILITY subparameter. Mapping which applications are defined to each FACILITY is a user-controlled option.

4.2.4 Broadcom Top Secret database files

The files used by Broadcom Top Secret to secure an environment are:

- Security file - an encrypted file that contains the security records of all user and resource permissions and restrictions
- Parameter file - a file that contains and defines Broadcom Top Secret Control Options used at initialization and sets up the operating environment
- Audit/Tracking file - a file that contains security-related events such as violations, job and session initiation, and resources accesses
- Backup file - a file that contains the Automatic Daily Backup of the Security File
- Recovery file - a file that contains recent administrative commands and can be used in conjunction with the backup file to restore a damaged security file.

4.3 Broadcom Top Secret subsystem interfaces

The interfaces discussed in this section provide Broadcom Top Secret access to z/OS subsystems.

TSO

Broadcom Top Secret provides the ability to control access to TSO, commands, and ISPF/PDF panels.

CICS

Broadcom Top Secret provides the ability to control access to CICS. Security access can be implemented at a transaction level or resource level.

Broadcom Top Secret implements a sign-on interface for CICS to further control the environment of the CICS user. The interface may include a new sign-on transaction name and a different sign-on panel.

IMS

Broadcom Top Secret provides the ability to control access to IMS. Security access can be implemented at a transaction level or resource level.

Db2

Broadcom Top Secret provides the ability to control access to Db2. When Broadcom Top Secret Security for Db2 is installed, native Db2 security is disabled. Db2 also provides a separate subsystem in the product for security.

5

RACF project overview

This chapter is intended as a project management guide for a Broadcom Top Secret to RACF conversion. It was written to give you a starting point from which to create a security project plan that is appropriate for your environment.

The information presented here was gathered from several Broadcom Top Secret to RACF conversions. The project examples represent a typical, generic project converting only one Broadcom Top Secret database to RACF, with expected completion within three to six months. The actual time it will take you to complete your migration will probably differ, depending on the nature and complexity of your project.

There is no guarantee that, for any particular conversion, the information contained in this manual is either complete, accurate, or even appropriate. Any individual security usually has tasks associated with it that are unique and specific to that particular migration. However, there are also many tasks that are common to all security migrations. The purpose of this document is to describe those tasks, and let you decide whether the task is appropriate for your particular migration.

Some of the tasks in a security project involve determining how other products, such as CICS, IMS and Db2, interface with RACF or Broadcom Top Secret. Whenever those tasks are discussed in this book, you are usually referred to the documentation of the other product. It would be difficult, if not impossible, to accurately maintain that kind of information in a manual of this type. Instead, this book concentrates on providing information not readily found in other sources, such as creating a security plan and giving you some practical guidelines for converting your Broadcom Top Secret database to an equivalent RACF database.

This chapter describes how to prepare for the project, build the project plan, and schedule the necessary resources. The need for assessing the current environment and suggested personnel skills are also discussed.

5.1 Preparing for the project plan

In order to build a good plan, you will have to review your Broadcom Top Secret database and supporting system environment for any security-related impacts. What you find will determine the number and types of people you need to find for the team. In addition, you must consider what type of education is needed, who would need it, and when it should be completed.

Your overall goal is to build as complete a plan as possible, using information from this book or other sources. The plan should identify all required tasks, who will do them, and when the tasks should be completed.

5.1.1 Review the current Broadcom Top Secret environment

The first step is to look at what security functions are implemented using the Broadcom Top Secret database. You will also need to decide how to convert the Broadcom Top Secret database, determine any impacts on the supporting system environment, and identify applications with security interfaces.

Assess the current Broadcom Top Secret database

Some features in Broadcom Top Secret do not convert easily or on a one-to-one correspondence to RACF. This is due to the fact that Broadcom Top Secret and RACF are two separate, individual products.

Typically, this means you have to examine each vendor product (for example, OEM) implemented in your environment and determine what has to be done, if anything, for each product to work with RACF. In most cases, each vendor's product documentation will have published RACF installation instructions and these should be reviewed. Identify all vendor product features you are using that RACF does not have an equivalent function for, then determine alternative ways of providing the same protection using RACF functions. Also, you have to check your z/OS base product code for any security-related Usermods, Accounting Exits, JES2 exits, and so forth.

As you assess the Broadcom Top Secret database and uncover potential issues, ask whether a current business need still exists which caused the original implementation of the security feature. If a need still exists, a solution should be found for converting the feature to the RACF environment. Many solutions can be found using either procedural controls or automated solutions.

Decide on how to convert the security database

You will have to create a RACF database that matches, as much as possible, your Broadcom Top Secret database. As part of this task, you have to write or obtain automated programs that can assist in converting the rules and parameters contained in the Broadcom Top Secret database to the appropriate RACF commands.

You have several choices here:

- You can buy an existing product to assist with the migration.
- You can write your own conversion routines.
- You can “start from scratch”, that is, instead of converting your current Broadcom Top Secret database, you build the RACF database with new definitions.

If you choose to convert your Broadcom Top Secret database, most likely you will have to write or obtain automated programs that can assist in database conversion. Typically, these programs or “tools” use the information in the Broadcom Top Secret database to create RACF commands. When these RACF commands execute, they load the appropriate security information into an empty RACF database.

The differences between the way Broadcom Top Secret and RACF protect resources, any database conversion will probably not be completely transparent. Therefore, it is very important that you ensure the RACF commands will implement the same or better access control integrity than the Broadcom Top Secret environment.

If you choose to write your own conversion programs, be aware that the programs may take several months to write. Keep in mind that they need to be ready before the start of unit testing. In addition, you should do several RACF database loads during the development phase in order to ensure an adequate amount of testing.

If you choose to obtain the conversion programs from other sources, ensure that you will be able to customize these programs to fit your individual needs.

> **Note:** It is very important that you understand the amount of work involved in converting your Broadcom Top Secret database. Several chapters of this book are devoted to this topic. You should review them thoroughly before making your decision.

Analyze the current system environment

You will need to complete a comprehensive, detailed review of any products, programs, or interfaces that perform security functions. Depending on what is being done, you may have to modify program code or write program code or exits which would perform the function on behalf of a user’s request.

To analyze your current system environment, s tart by listing all hardware and software products you have installed. Identify which ones have security interfaces, or may otherwise be affected by this conversion. (This research is similar to what you might do in preparation for a systems software upgrade, such as a ServerPac Installation.)

For each product that has a security interface, determine how RACF can provide the same protection. Also determine the amount of work required to have the product work with RACF, instead of Broadcom Top Secret.

Preparing the RACF test system

A test system, similar in size and nature to one that might be used for an z/OS software upgrade, has to be available for the project.

You need the RACF test system on a “dedicated” basis for about two to three months to complete this project in a timely and efficient manner. By a “dedicated” test system, we mean one that is available during the normal working day so that the project team can work on the environment during their normal day-to-day work schedule.

Typical Test System requirements include:

- A SYSRES volume to install RACF
- DASD space for the RACF database
- DASD space for the applications to be tested under RACF

In some cases, because of system constraints, the only test system you can dedicate to the project may not be large enough to handle the testing of more than one application at a time. While this will allow you to do not much RACF testing, you will eventually have to test RACF using a second, more comprehensive test system. You will probably not be able to dedicate this second test system to the project.

You have to install RACF typically on a test system that is separate from the broadcom Top Secret production system. You will most likely not have to upgrade or install any product for the sole purpose of using RACF. However, some of the advanced functions of RACF may work only with the higher release levels of some products.

5.1.2 Personnel

A typical security project involves people with the following generic job descriptions. Most people working on migrations usually perform multiple duties throughout the project. As you determine which tasks need to be done, also determine how many people are needed to perform the tasks, in order to ensure a successful migration.

Sample project organization describes the organization that should be implemented prior to the beginning of a migration.

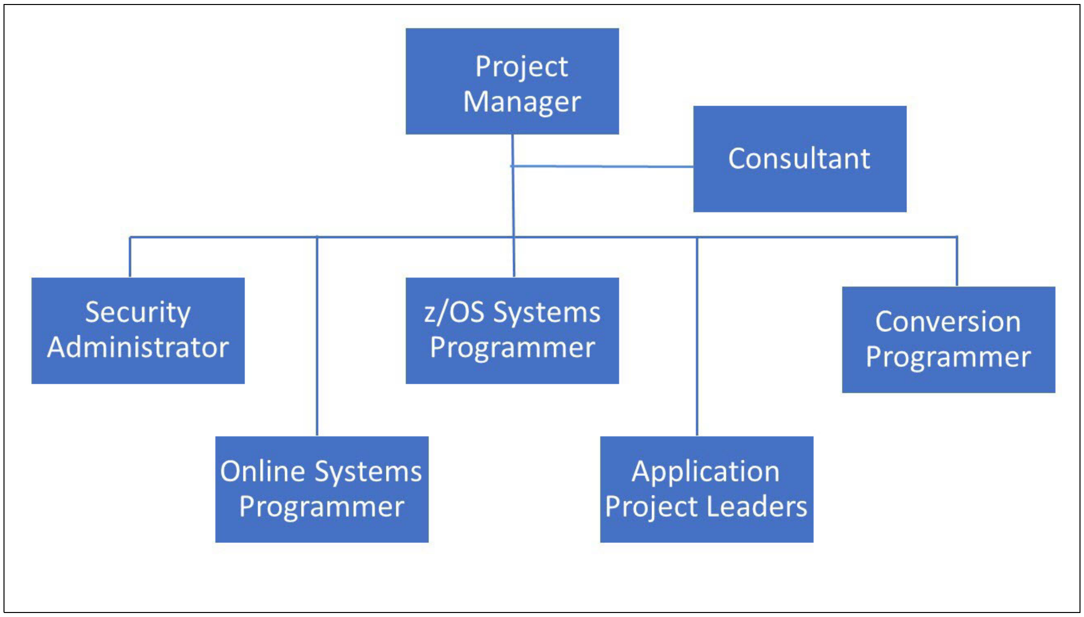


Figure 5-1 Sample project organization

The security administrator

The security administrator is usually the most important and busiest person in a security migration. This person is the focal point for all questions related to what protection is currently in effect and why it was originally implemented. The administrator also determines the methodology and customizing of the conversion programs that convert the Broadcom Top Secret database to RACF.

Frequently the administrator is also responsible for coordinating all testing, updating all security procedures, and educating end users in RACF. Many responsibilities the administrator has regarding technical issues, this person is usually too busy to be the project manager.

A key factor to the success of any project is having a security administrator on the team who knows why past decisions were made and can provide guidance on whether current business needs exist for carrying functions into the RACF environment.

The project manager

The project manager is primarily responsible for creating the plan, with the assistance of the team, and for monitoring the progress of the project. Since the team usually consists of people from several departments, the project manager has to make sure everyone is committed to performing and completing the tasks he or she is responsible for throughout the project. This person is responsible for acquiring any additional personnel or systems support necessary to keep the project on schedule. The project manager may also assist the security administrator in his tasks.

The conversion programmer

The conversion programmer is responsible for configuring the options of the conversion programs. This programmer coordinates resolution of database conversion issues and configures the conversion programs to properly represent the desired RACF result.

The z/OS systems programmer

The main responsibilities of the z/OS systems programmer are to install and customize RACF, to create and maintain the test system to be used throughout the conversion, and to assist in the testing of RACF.

In some cases, the z/OS systems programmer also installs and customizes the company's use of vendor (OEM) program products which use security interfaces. Vendor product documentation usually contains specific instructions on how to set up their product to use RACF.

The online systems programmers

Online systems programmers are responsible for performing whatever work is necessary so that their subsystems work properly when RACF is installed. This typically means analyzing their current subsystem for interfaces to Broadcom Top Secret, preparing the appropriate code and JCL to accomplish the same protection under RACF, and assisting in the RACF testing. Some examples of subsystems are TSO, IMS, CICS, Db2 or VTAM.

The application project leaders

Application project leaders are responsible for verifying that they are the true owners of any resources (usually data sets) as identified through the Broadcom Top Secret database, and ensuring adequate testing of their applications. During the testing phase, they are responsible for determining that the security protection for their resources under RACF is acceptable, and that their applications function as well or better than they did with Broadcom Top Secret.

5.1.3 Education

You need to determine who must receive RACF education before the project starts, when the education should be completed, and which classes should be attended. This education could include formal IBM-taught classes, self-study courses, or classes you may develop in-house for help desk or end-user training. You should schedule and attend RACF education for performing day-to-day administration prior to starting the project.

5.2 Building the project plan

This task simply means documenting all the tasks that have been identified, who is to do them, and when they are to be done. Once you have decided you *want* to convert to RACF, you then have to determine what methodologies to use in converting to RACF. You need to develop a detailed plan which identifies the tasks to be performed, who are the most qualified to complete the task, and a projected time frame. Remember to include items that are not pure tasks, such as educational needs and test system availability.

To create accurate estimates for the work involved in some of the tasks, analyze what it will take to complete that particular task. Remember, there can be multiple items to perform in order to finished the project tasks. Ask the same questions for any other significant software installed on the Broadcom Top Secret system. The following is an example of a potential project task.

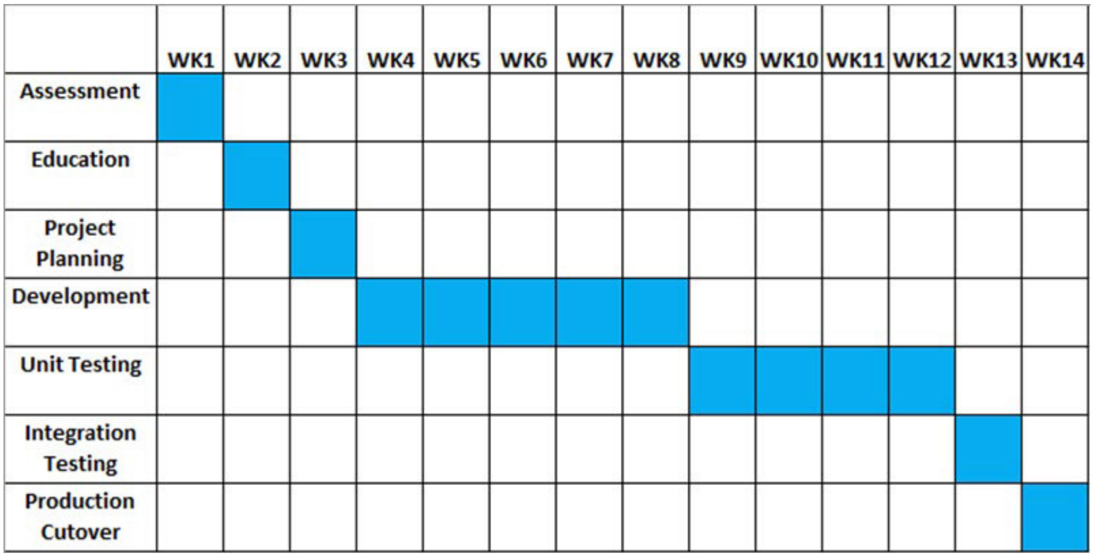
You, as project manager, review the list of software installed on your system and see that CICS is one of the products installed. You ask the CICS systems programmer the following questions:

1. Are there any “non-standard” uses of security that would interfere with a migration to RACF?
2. How much work would be involved in converting the security for the CICS regions to RACF?

If the answer to the first question is yes, then that is identified as a potential migration issue. Also, the amount of overall work involved in converting CICS security to RACF, and who will do that work, is identified in the plan. You will not begin that work until you have determined that the issue identified in the first question will not cause a delay in the overall project.

In all cases, determine whether a current business need exists for the project task. If something was done in Broadcom Top Secret which does not need to be carried forward into the RACF environment, then this item does not need to be addressed.

Figure 5-2 shows a typical project plan by phase lasting over 14 weeks. There are seven major phases to the migration project: assessment, education, project planning, development, unit testing, integration testing and production cutover.



	WK1	WK2	WK3	WK4	WK5	WK6	WK7	WK8	WK9	WK10	WK11	WK12	WK13	WK14
Assessment	■													
Education		■												
Project Planning			■											
Development				■	■	■	■	■						
Unit Testing									■	■	■	■		
Integration Testing													■	
Production Cutover														■

Figure 5-2 Project planning phase items

5.2.1 Significant project tasks

The following project tasks will be involved.

Analyze the current security environment

Examine the security database and system environment to identify which technical issues need to be addressed. This includes database features which do not have a direct RACF functional equivalent and any system exits or product interfaces which perform security functions. Review all issues against whether a current business need exists.

Project management

Throughout the project, you have to monitor and adjust the plan you created at the beginning of the project.

Planning

In this phase, a detailed project plan is developed for the remainder of the project. It lists who is to be involved, what other resources are needed, all the security interfaces currently in effect, and any issues that have to be resolved before proceeding to the next phase. Typical significant checkpoints would be the initial load of the RACF database, testing and cutover.

Identify project team

Identify the people who will complete the tasks identified in the project plan.

Identify major concerns or system changes

Review all conditions or situations that were identified as potential issues. Determine whether any of them are serious enough to warrant delaying the project until the condition or situation in question is resolved. Also, make sure you coordinate with other projects in the company, such as software upgrades or hardware installations, that could interfere with the schedule for this project.

You have to identify anything that could be interpreted as a significant technical project issue. You need to identify any issue which would adversely affect the project time frame. You want to avoid putting a lot of effort into the if a condition exists that will cause you to delay the project anyway. For example, if the necessary test system is not going to be available for several months, there is no need to have the online systems programmers preparing their products for RACF.

In many cases, you will need the support and approval of the end-user community before beginning this project. Often, the information from this phase is used to help obtain that support and approval.

Install and customize RACF

You have to install RACF, typically on a test system apart from the production system that contains Broadcom Top Secret. You also have to review the customizing options available, and determine what would be appropriate for your environment.

Prepare the RACF test environment

In this phase, you prepare a RACF test environment that emulates the Broadcom Top Secret environment. All the security interfaces that exist in the current system are identified. Any code that has to be prepared to accomplish the same protection under RACF is prepared in this step.

Install conversion programs

In this phase, install the conversion programs to be used to convert Broadcom Top Secret to RACF. These programs should be customized based on your specific requirements.

Review naming conventions

Naming conventions are important, because high-level qualifiers of data sets play a more important role in RACF than they do in Broadcom Top Secret. RACF assigns ownership of data sets according to a high-level qualifier. Only one RACF group can “own” a high-level qualifier at any one time. For example, Broadcom Top Secret allows the use of generic characters for masking of high-level qualifiers, while RACF does not.

Review security procedures

Identify all procedures that will change due to the to RACF. Typical procedures of this type include how help desk personnel are to change passwords, or how operators and software automation products interact with RACF and z/OS operations.

RACF group structure planning

This is a very important part of the database conversion. You want to build a RACF group structure which is manageable, well-designed, and meets your specific needs. For example, there are certain Broadcom Top Secret `logonid` fields which provide security administrative functions and the migration team needs to decide how to provide similar functionality to the RACF community through centralized or distributed security administration procedures.

Convert the security database

In this phase, you run your conversion programs to convert the Broadcom Top Secret database to RACF commands. Through repetitive executions of the tool against the Broadcom Top Secret database, you should be able to build a functionally equivalent RACF database. Final testing should verify the integrity of the user ID and resource profile definitions.

Testing

A typical RACF testing sequence, or “cycle”, might be:

- Create a RACF database to match the Broadcom Top Secret database.
- IPL the test system with RACF.
- Execute the test plans.
- Review the results.
- Make any corrections to the conversion programs.
- Retest the system.

Several testing cycles are usually needed before your RACF environment is ready for testing against the full production system. This usually takes several weeks of effort.

Unit testing

Unit testing tasks concentrate on verifying the initial RACF database, system Environment and selected important applications. You identify any differences between the old and new security environments, make any necessary corrections, and retest until you’re satisfied.

Integration testing

In this phase, you test your RACF environment against the full production system. You also target major applications within the company to verify their current functionality has not been adversely impacted. This is usually done on weekend “graveyard” shifts. If there are no major problems during this phase, you are ready to convert to RACF.

Develop a backout plan

It would be prudent to develop a backout plan in case you need to back out RACF and return to the Broadcom Top Secret environment. The backout plan typically identifies all exits and interfaces that were replaced, how to reinstall them if necessary, and relinking to the Broadcom Top Secret databases. Each project team member responsible for implementing changes for the RACF needs to provide input into the overall backout plan.

Another option is to publish a set of items, or expectations, which would potentially trigger a backout. Some examples include inadequate testing of security functions and applications not converted to use RACF. These expectations should be communicated to all affected users prior to the cutover date.

Preserve the Broadcom Top Secret databases

Prior to the cutover date, make copies of the Broadcom Top Secret security databases. Problem resolution will be critical during the days immediately following the cutover, and access to the previous security environment could help resolve user and system issues.

Once the migration to RACF has been completed, you may need to check user access problems against what the access was in Broadcom Top Secret. Since you may not have the ability to log on to Broadcom Top Secret, you must have the LIST(ACID) reports for all ACIDs available, or any other report used to diagnose and solve user access problems. These files and/or reports can be written to DASD files as part of the cutover process for easy accessibility.

You could also migrate Broadcom Top Secret to your test environment concurrent with the RACF production environment cutover. You could then log on to Broadcom Top Secret to quickly resolve problems.

Production cutover

Before migrating RACF to production, you probably want to test RACF with the full production system, similar to the way you might test an z/OS software upgrade before putting it into production.

Successful migrations freeze all changes to Broadcom Top Secret shortly before the cutover weekend. The conversion tool is run one last time and a final RACF database is built. All modified exits and interfaces are installed and passwords are synchronized.

5.3 Resource scheduling

You need to decide how and when to allocate your project team skills across the entire project. Table 5-1 is a representative sample of the typical resources needed by project phase and the level of effort required. Each of the six project skills has responsibilities in each project phase.

In this table, the full-time or part-time designation represents the allocation of time on the project in relation to their overall job responsibilities. For example, if the teammate can work 20 hours per week on the project, then a full designation would mean 20 hours of level-of-effort.

Table 5-1 Scheduling graph

Resource type	Assessment	Education	Planning	Development	Unit Testing	Integration Testing	Production Cut-over
Project manager	Full	Full	Full	Part	Part	Full	Full
Security administrator	Full	Full	Full	Part	Part	Full	Full
z/OS systems programmer	Full	Full	Part	Full	Part	Full	Full
Conversion programmer	Full	Full	Part	Full	Part	Part	Part
Online systems programmer	Full	Part	Part	Full	Part	Full	Full
Application project leaders	Full	Part	Part	Part	Part	Full	Full

5.4 Summary

In summary, the success of the project will depend on the quality of the project plan and the deployment of the right project team members with the right skill level at the right time. Here are some additional considerations.

Management involvement

You need strong management commitment to undertake a major migration of any kind. Owners or managers of production applications, in particular, must be involved in testing phases. This is an additional task for these people and there must be sufficient management commitment to force testing compliance on a reasonable schedule.

Test system

It is not practical to run both Broadcom Top Secret and RACF on the same z/OS system. Likewise, it is not practical to undertake a migration to RACF without having a RACF system available for testing. In this case “testing” means a large range of testing and this is not practical on any production system. Therefore, you need a RACF z/OS system to use solely for test purposes.

In practice the test system is most likely to be a Logical Partition (LPAR) on a larger processor. With some care, the test z/OS can share DASD with your production data, making testing much easier. Whether you clone your production z/OS (removing Broadcom Top Secret and installing RACF), or install a new z/OS (with RACF already integrated) is your choice. In either case, systems programming time is needed to install, make ready, and maintain the test z/OS system.

Education

You can obtain a reasonable overview and understanding of RACF by reading the RACF manuals. This is sufficient for many purposes. However, if you are the project manager, or intend to be the primary RACF specialist in the organization, you should arrange for formal RACF education.

Application involvement

A major goal of the project is to avoid disruption of production applications and this can be accomplished only with sufficient testing. Major applications can be complex, with many jobs, files, procedures, and programs involved. Specific job and application knowledge is usually required to test these applications, and this means involvement by the application groups. They must help you test their applications in the new RACF Environment.

Manpower and timing considerations

For a security subsystem to be effective, it must be very tightly tied into the heart of the operating system. Given this, it is quite difficult to make a major change in the security subsystem without impacting system production. A large, production z/OS installation has many complex jobs. Some of these are rarely used, such as year-end jobs or obscure recovery jobs.

The bulk of basic Broadcom Top Secret user records and resource rule records can be automated. However, testing the results of this conversion and discovering/migrating all the special cases that exist, without disrupting production, is another matter altogether. Nevertheless, this is the requirement for almost all Broadcom Top Secret to RACF migrations. It is these practical considerations that dictate the resources and manpower needed for migration.

No single plan can apply to all situations. However, a project plan of three to six months, with one full-time person and several part-time people working on the project, is typical.

6

Database migration

This chapter describes the process of the actual database migration of Broadcom Top Secret to IBM’s RACF. It provides guidance on how to convert a certain Broadcom Top Secret function to the equivalent function in IBM’s RACF.

6.1 Conversion methodology

This section discusses some of the issues and approaches that can be used when converting your Broadcom Top Secret database to RACF. Like Broadcom Top Secret, RACF offers a number of ways of implementing security policies and procedures. Experience has shown that some approaches work better than others. This section provides a number of recommendations for designing and implementing a conversion methodology from Broadcom Top Secret to RACF.

6.1.1 Migration considerations

The migration from Broadcom Top Secret to RACF involves more than a conversion of database records. We must first note that this is an excellent time (just before your migration) to review, rethink, and polish your security policy. A clear vision of what you want to produce will help the migration work and provide better results. Some of the key elements to a migration are discussed in “RACF project overview” on page 45. Before you begin the conversion, you must have a plan that includes:

- Management involvement, signoff, support
- Test system
- Education
- Application involvement
- Manpower and timing

One of the lasting aphorisms of the data processing business is “Garbage In - Garbage Out,” commonly known as GIGO. While it is a complex, one-time activity, migrating a security database from one product to another is a data processing function, especially when an automated tool is used to help perform part of the work. A fairly clean input database at the beginning of the migration will help produce a higher quality result. There is no magic in the migration process or tools that will automatically clean up substantial problems in the initial database.

Unless meticulously maintained, a security database tends to accumulate a certain amount of unwanted or erroneous entries over time. There are a number of causes: changing security administrators, changing philosophy of security management, former users who still own resources, and so forth. You have several choices for handling these problems:

- Make a reasonable effort to clean up your original database, before starting the migration process.
- Migrate whatever is in your original database, and clean up the resulting RACF database.
- Ignore the problems, and accept whatever appears in the final RACF database.

The first choice is usually the best one. You understand your current Broadcom Top Secret database and have the skill to review it. While reviewing and correcting a large security database is not an enjoyable task, it will certainly reduce future problems. Some migration tools may help you clean up your current database.

Schedule pressures may push you toward the second choice- migration. The problem with this approach is the cleanup after migration. The migration process may amplify the problems in the original database. The conversion of a Broadcom Top Secret database to a RACF database is not a simple, one-to-one process. Small anomalies in the input, easily corrected if someone would take the time to do it, might create large unwanted structures in the output.

A pre-conversion review process should be considered (and correct) obvious errors in the database. It should also consider design and philosophical changes that will produce a better database after migration. Again, small changes here may make the migration much easier and produce a better result. Examples of such changes are the elimination of FACILITIES that are not really needed or that are outdated.

In practice, of course, you are likely to use all three choices: some clean up of the original database, some clean up of the RACF database, and then go into production with the resulting database.

6.2 Converting ACIDs

ACIDs in Broadcom Top Secret become the user IDs and groups that make up the RACF security environment. Table 6-1 shows examples of ACIDs in Broadcom Top Secret and their RACF equivalents.

Table 6-1 ACIDs conversion table

Broadcom Top Secret Terms	RACF Equivalent
Zones	GROUPs
Divisions	GROUPs owned by Zone
Departments	GROUPs owned by Division
Profiles	GROUPs owned by a Division or Department
Users	USERs
SCAs	USERs with SPECIAL privilege
LSCAs	USERs with some special privileges
VCAs	USERs with group special privileges
DCAs	USERs with group special privileges
ZCAs	USERs with group special privileges
The ALL record	UACC (universal access authority) or ID(*) rules

6.2.1 Broadcom Top Secret user/group migration issues

Migrating the basic user from Broadcom Top Secret to RACF isn’t necessarily a complex task. What may become more complicated is the migration of some user privilege attributes. Some of these privileges can be carried across into RACF, while there are a few that will require careful planning and possibly an exit. We have tried to keep this section focused on some fairly common areas.

The conversion process is shown in Figure 6-1.

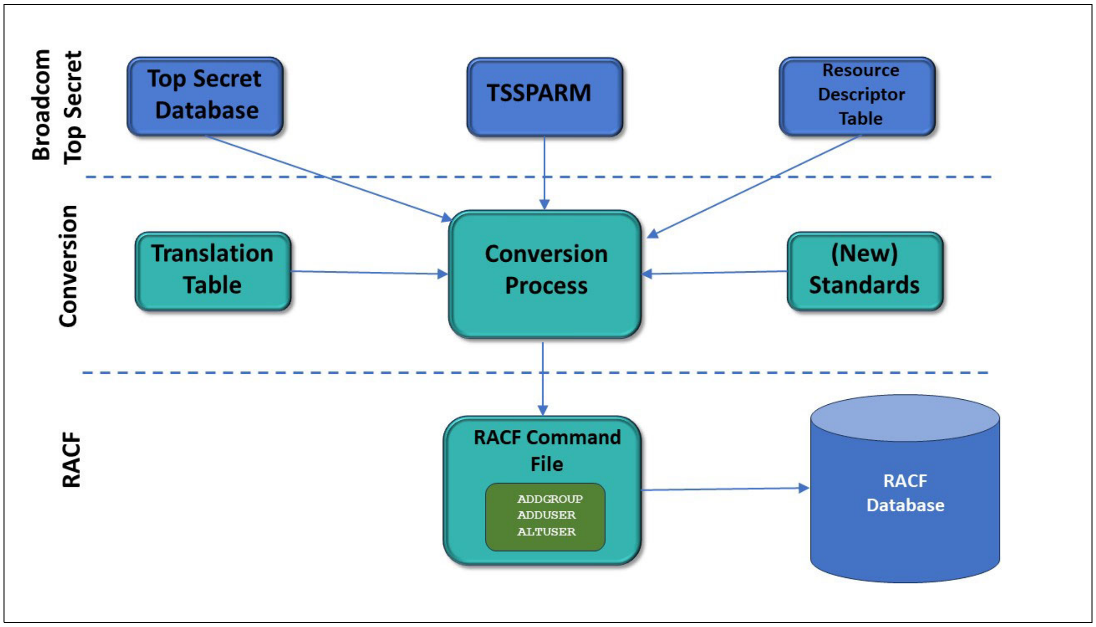


Figure 6-1 Security database conversion process

An essential piece of the conversion process is the selection of a RACF administrative group structure. The structure is usually based on the Broadcom Top Secret structure. The RACF structure should allow for user administration and user access authorization.

The flow of ACID conversion may be:

1. Design and define a set of new naming standards for the RACF database.
2. Design and define the RACF group structure (see Chapter 5, “RACF project overview” on page 45).
3. Run LIST commands against the Broadcom Top Secret database which lists all ACIDs into a data set.
4. Use the output from the report as an input to the conversion process.
5. Output from the conversion process is a set of RACF commands written to a data set. These commands define group profiles and user profiles, as well as user-to-group connections.
6. Use the commands to load the new RACF database.

6.2.2 Listing the Broadcom Top Secret ACIDs

The following Broadcom Top Secret commands can be used to generate reports that list all ACIDs, as well as the resources each ACID can access:

```
Profiles:
   Zones          - TSS LIST(ACIDS) DATA(ALL) TYPE(ZONE)
   Divisions      - TSS LIST(ACIDS) DATA(ALL) TYPE(DIV)
   Departments    - TSS LIST(ACIDS) DATA(ALL) TYPE(DEPT)
   Profiles       - TSS LIST(ACIDS) DATA(ALL) TYPE(PROF)
   Users          - TSS LIST(ACIDS) DATA(ALL) TYPE(USER)
Security Administrators:
   System         - TSS LIST(ACIDS) DATA(ALL) TYPE(SCA)
   Limited Scope  - TSS LIST(ACIDS) DATA(ALL) TYPE(LSCA)
   Division       - TSS LIST(ACIDS) DATA(ALL) TYPE(VCA)
   Department     - TSS LIST(ACIDS) DATA(ALL) TYPE(DCA
   Zone           - TSS LIST(ACIDS) DATA(ALL) TYPE(ZCA)
The All Record - TSS LIST(ALL)
```

Typically, you would write these reports to DASD files, then process the information in them using a conversion tool providing automated processing via application programs or REXX execs.

6.2.3 Reviewing and defining ACIDs to RACF

For each Broadcom Top Secret ACID, we must determine:

- What the equivalent RACF definition is
- What appropriate RACF command to use when converting

The commands shown in Table 6-2 are used to define the ACIDs to RACF.

Table 6-2 ACID to RACF definitions

Broadcom Top Secret Term	RACF Equivalent
Zones	ADDGROUP
Divisions	ADDGROUP
Departments	ADDGROUP
Profiles	ADDGROUP
Users	ADDUSER
SCAs	ADDUSER
VCAs	ADDUSER
DCAs	ADDUSER
ZCAs	ADDUSER

Converting zone, division and department ACIDs

As in Broadcom Top Secret, every user must initially “belong” somewhere. In Broadcom Top Secret, they are usually defined to a department. In RACF, the Broadcom Top Secret departments become what RACF refers to as “administrative groups”. These groups become the default groups when users are defined to RACF. Zone and division ACIDs become the group tree structure which allows administrative controls.

Listing zone, division and department ACIDs

Example 6-1 shows how to list the zone, division and department ACIDs, along with the output generated by each list command:

Example 6-1 Listing zone, division and department ACIDs with output

```
Command:
TSS LIST(ACIDS) DATA(ALL) TYPE(ZONE)
Output:
ACCESSORID = ZONE1     NAME   = ZONE ONE
TYPE       = ZONE      FACILITY   = *NONE*
CREATED    = 04/20/98  LAST MOD   = 04/20/21
```

```
ACIDS      = DIV1(V)
Command:
TSS LIST(ACIDS) DATA(ALL) TYPE(DIV)
Output:
ACCESSORID = DIV1      NAME       = DIVISION ONE
TYPE       = DIVISION  FACILITY   = *NONE*
CREATED    = 04/20/92  LAST MOD   = 04/20/21
ACIDS      = DEPT1(D)
Command:
TSS LIST(ACIDS) DATA(ALL) TYPE(DEPT)
Output:
ACCESSORID = DEPT1     NAME       = DEPARTMENT ONE
TYPE       = DEPT      FACILITY   = *NONE*
DIV ACID   = DIV1      DIVISION   = DIVISION ONE
CREATED    = 04/20/92  LAST MOD   = 04/20/21
ACIDS      = PROF1(P)
```

Defining zones, divisions and departments to RACF

To convert these ACIDs, we define them to RACF as GROUPs, using the ADDGROUP command. ZONE1 becomes a group owned by SYS1 if ZONEs exist. If not, this level is skipped. DIV1 becomes a group owned by SYS1 if no ZONEs exist, or by ZONE1 if there are zones. DEPT1 becomes a group owned by DIV1:

```
ADDGROUP (ZONE1)   SUPGROUP(SYS1)  OWNER(SYS1)
ADDGROUP (DIV1)    SUPGROUP(SYS1)  OWNER(SYS1)
or ADDGROUP (DIV1) SUPGROUP(ZONE1) OWNER(ZONE1)
ADDGROUP (DEPT1)   SUPGROUP(DIV1)  OWNER(DIV1)
```

Note: Broadcom Top Secret allows you to define ACIDs starting with numerics, such as DIV=123DIV. In RACF, a group must start with an alphabetic character. If you have used this feature, the ACID names will need to be changed.

6.2.4 Converting profile ACIDs

Conversion of Broadcom Top Secret profiles is a little more complex due to the differences in philosophy of the two products.

Broadcom Top Secret profiles become what RACF refers to as “functional groups”. Both products use this concept in the same way. Typically, all resources needed to perform a particular function are permitted to the same Broadcom Top Secret profile (or RACF functional group), rather than to each individual user performing that function. Each product has a way of associating the right users with the right Broadcom Top Secret profiles or RACF functional groups.

In Broadcom Top Secret, the *profile* consists of the resources common to a group of users and is permitted to each user needing the resources. In RACF, the *functional group* is a list of users who will access the same set of resources. Converting the resources in a Broadcom Top Secret profile to the RACF resource will be covered in this section.

This section is concerned with converting the profile to a RACF group and ensuring the users who had the profile are connected to the functional group.

In RACF, functional groups usually do not “own” any users; that is, no users have these groups as their default group. users instead are connected to these groups in order to access the resources that these functional groups are permitted to use.

The term *profile* has a different meaning in RACF than the Broadcom Top Secret definition. The profile in RACF is simply a record in the database. You can have group profiles, user profiles, data set profiles, etc. Refer to the *z/OS Security Server (RACF) Security Administrator’s Guide, SA23-2289* for the precise definition of the term as used by RACF.

Listing profile ACIDs

Example 6-2 shows how to list the Broadcom Top Secret profile ACIDs, along with an example of the output:

Example 6-2 List profile ACIDs with output

```
Command:
TSS LIST(ACIDS) DATA(ALL) TYPE(PROF)
Output:
ACCESSORID = PROF1     NAME       = PROFILE ONE
TYPE       = PROFILE   FACILITY   = *NONE*
DEPT ACID  = DEPT1     DEPARTMENT = DEPARTMENT ONE
DIV ACID   = DIV1      DIVISION   = DIVISION ONE
CREATED    = 04/20/98  LAST MOD   = 04/20/21
XA DATASET = SYS1.                              OWNER(SYS1)
ACCESS     = UPDATE
ACIDS      = USER1      SCA1    (S) VCA1    (V) DCA1    (D)
ACCESSORID = PROF2     NAME       = PROFILE TWO
TYPE       = PROFILE   FACILITY   = *NONE*
DIV ACID   = DIV2      DIVISION   = DIVISION TWO
CREATED    = 05/21/98  LAST MOD   = 04/20/21
XA DATASET = SYS2.                              OWNER(SYS1)
ACCESS     = READ
ACIDS      = USER3
```

Defining profile ACIDs to RACF

To convert the profile ACIDs, we define them to RACF as *groups* using the ADDGROUP command. In the previous examples, PROF1 becomes a group owned by DEPT1 and PROF2 becomes a group owned by DIV2:

```
ADDGROUP (PROF1) SUPGROUP(DEPT1) OWNER(DEPT1)
ADDGROUP (PROF2) SUPGROUP(DIV2 ) OWNER(DIV2 )
```

In addition, all resources that these Broadcom Top Secret profiles could access are defined to RACF and the function group (e.g., PROF1) is permitted to the resource definition. All users who were associated with these Broadcom Top Secret profiles are connected to the corresponding RACF functional groups with the CONNECT command:

```
CONNECT USER1  GROUP(PROF1) OWNER(PROF1)
CONNECT SCA1   GROUP(PROF1) OWNER(PROF1)
CONNECT VCA1   GROUP(PROF1) OWNER(PROF1)
CONNECT DCA1   GROUP(PROF1) OWNER(PROF1)
CONNECT $USER3 GROUP(PROF3) OWNER(PROF3)
```

6.2.5 Converting user ACIDs

You normally convert each Broadcom Top Secret user ACID to a RACF user ID.

Listing user ACIDs

Example 6-3 shows how to list user ACIDs, along with an example of the output:

Example 6-3 List user ACIDs with output

```
Command:
TSS LIST(ACIDS) DATA(ALL) TYPE(USER)
Output:
ACCESSORID = $USER3       NAME              = AARON AARDVARK
TYPE       = USER         SIZE              = 768  BYTES
DEPT ACID  = DEPT1        DEPARTMENT        = DEPARTMENT ONE
DIV ACID   = DIV1         DIVISION          = DIVISION ONE
ZONE ACID  = ZONE1        ZONE              = ZONE ONE
CREATED    = 11/11/99     LAST MOD          = 24/03/21 12:34
PROFILES   = PROF1    PROF7
GROUPS     = OMVSGRP
LAST USED  = 25/03/00 13:26 CPU(CPU1) FAC(TSO     ) COUNT(00645)
DFLTGRP    = OMVSGRP
MYDEFINE   = MYDATA
----------  SEGMENT CICS
OPIDENT    = ABC
----------  SEGMENT OMVS
HOME       = /
OMVSPGM    = /bin/sh
UID        = 0000009303
----------  SEGMENT TSO
TSOCOMMAND = LOGOFF
TSOLACCT   =  ACCT123
TSOLPROC   = PROCSP
TSOLSIZE   = 0000000
TSOOPT     = NOMAIL,NONOTICES,NOOIDCARD
XA DATASET = SYS1.                                OWNER(SYS1)
ACCESS     = UPDATE
INSTDATA   = THIS IS AN EXAMPLE OF INSTALLATION DATA
```

Defining users to RACF

The user ACIDs are defined to RACF as USERs using the ADDUSER Command. The default group is the division or Department the user belonged to in Broadcom Top Secret. Also, as described in converting profile ACIDs, if there were any Broadcom Top Secret profiles listed in the ACID, the user will be connected to the equivalent functional group in RACF using the CONNECT command. The TSO, CICS and OMVS segments will be added to the user ID as they are in Broadcom Top Secret. Therefore, to define the user listed in Example 6-3 to RACF, we would enter the following commands:

```
ADDUSER $USER3 DFLTGRP(DEPT1) OWNER(DEPT1) NAME(‘AARON AARDVARK’) -
DATA(‘THIS IS AN EXAMPLE OF INSTALLATION DATA’) -
TSO(PROC(PROCSP) ACCTNUM(‘ACCT123’)COMMAND(LOGOFF)) -
CICS(OPIDENT(ABC)) -
OMVS(HOME(/) PROGRAM(‘/bin/sh’) UID(0000009303))
CONNECT $USER3 GROUP(PROF1)
```

Note: There are special considerations for OMVS segments; they are covered in “z/OS UNIX considerations ” on page 83.

Table 6-3 lists some of the Broadcom Top Secret ACID and resource rules that are subparameters of the RACF ADDUSER command. The RACF default group can be either the DEPT or DIV ACID:

Table 6-3 USER ACID parameter conversion

Broadcom Top Secret parameter	ADDUSER subparameter
ACCESSORID = USER1	ADDUSER USER1
NAME = ARRON	NAME(‘ARRON’)
INSTDATA = xxx	DATA(xxx)
ATTRIBUTES = SUSPEND	REVOKE
DEPT ACID = YYY	DFLTGRP(YYY)
DFLTGRP = OMVSGRP	DFLTGRP(OMVSGRP)
Segment OMVS	OMVS(parameters)
Segment CICS	CICS(parameters)
Segment TSO	TSO(parameters)

6.2.6 Converting security administrator ACIDs

RACF privileges are easy to identify, understand, and administer, but they are not as granular as Broadcom Top Secret privileges. Conversely, the Broadcom Top Secret privileges allow more granular control of authority, but have more complex interactions and may require more administrative effort. This section discusses the privileges we consider most important for user conversion.

Security administrators are defined as users in RACF. In addition, they are given the SPECIAL attribute, which denotes them as having the special privileges and authority typically associated with security administrators. The functions the administrator is required to perform will determine any additional required parameters (for example, CLAUTH if the user will have authority over selected user IDs.)

Listing security administrator ACIDs

Example 6-4 shows how to list system, zone, division and department security administrators, with examples of the output:

Example 6-4 List system, zone, division, and department security administrators with output

```
Command:
TSS LIST(ACIDS) DATA(ALL) TYPE(SCA)
Output:
ACCESSORID = SCA1      NAME       = MASTER SECURITY
TYPE       = CENTRAL   FACILITY   = BATCH,STC,TSO
CREATED    = 04/20/92  LAST MOD   = 04/20/21
PROFILES   = PROF1
ATTRIBUTES = CONSOLE
BYPASSING  = NODSNCHK,NOVOLCHK
```

```
XA DATASET = SYS1.                              OWNER(SYS1)
ACCESS     = UPDATE
----------  ADMINISTRATIVE AUTHORITIES
RESOURCE   = INFO
LIST DATA  = *ALL*,PROFILES
Command:
TSS LIST(ACIDS) DATA(ALL) TYPE(VCA)
Output:
ACCESSORID = VCA1      NAME       = DIV SEC ADMIN
TYPE       = DIV  C/A  FACILITY   = BATCH,STC,TSO
DIV ACID   = DIV1      DIVISION   = DIVISION ONE
CREATED    = 04/20/92  LAST MOD   = 04/20/21
PROFILES   = PROF1
ATTRIBUTES = CONSOLE
XA DATASET = SYS1.                              OWNER(SYS1)
ACCESS     = ALL
----------  ADMINISTRATIVE AUTHORITIES
FACILITIES = *ALL*
MISC1      = SUSPEND
Command:
TSS LIST(ACIDS) DATA(ALL) TYPE(DCA)
Output:
ACCESSORID = DCA1      NAME       = DEPT SEC ADMIN
TYPE       = CENTRAL   FACILITY   = BATCH
DEPT ACID  = DEPT1     DIVISION   = DEPARTMENT ONE
DIV ACID   = DIV1      DIVISION   = DIVISION ONE
CREATED    = 04/20/92  LAST MOD   = 04/20/21 PROFILES   = PROF1
XA DATASET = SYS1.                              OWNER(SYS1)
ACCESS  = ALL
----------  ADMINISTRATIVE AUTHORITIES
ACID       = *ALL*
ACCESS  = NONE
```

Defining security administrators to RACF

The ACIDs shown in Example 6-4 are defined to RACF as USERs. The SPECIAL attribute is used in RACF to distinguish users who will be performing security administrator functions. The SCA is the easiest because they convert to system SPECIAL which allows FULL administration of the RACF database. ZCA, LSCA, VCA and DCA users have restricted privilege and will be given a GROUP-SPECIAL attribute in RACF. Users who have the GROUP-SPECIAL attribute are restricted to only the RACF profiles that are within the scope of their groups.

There is a slight distinction between the way you add a user with the system SPECIAL attribute, and the way you add a user with the GROUP-SPECIAL attribute. In the following example, SCA1 is a user with system SPECIAL authority, and VCA1 and DCA1 are users with GROUP-SPECIAL authority:

```
ADDUSER SCA1 DFLTGRP(SYS1) SPECIAL
ADDUSER VCA1 DFLTGRP(DIV1) CLAUTH(USER)
CONNECT VCA1 GROUP(DIV1) SPECIAL
ADDUSER DCA1 DFLTGRP(DEPT1)
CONNECT DCA1 GROUP(DEPT1) SPECIAL
```

Security administrators perform the same basic functions in both products. However, the way each product defines those functions, in terms of resource rules and privileges, is completely different.

You should not attempt to map the attributes associated with the Broadcom Top Secret security administrators on a one-to-one basis to RACF. Instead, you have to understand what privileges you can assign to RACF security administrators, and what RACF commands are available to do that. The information you need to do this is in the *z/OS Security Server RACF Security Administrators Guide,* SA23-2289.Table 6-4 lists some of the RACF translations for the Broadcom Top Secret privileges that can be reviewed.

Table 6-4 User administration responsibilities

Broadcom Top Secret	RACF
MSCA, SCA	System SPECIAL
ZCA, VCA, DCA w/ full user responsibility	GROUP-SPECIAL w/ CLAUTH(USER)
Password only across the system	FACILITY IRR.PASSWORD.RESET access
Data Set rules responsibility	GROUP-SPECIAL to Data Set groups
Segment responsibility	FIELD level access to the required segments

6.2.7 Password

For conversion purposes, you must decide if you want to keep the same password across the conversion or if you want to change passwords for all the users. Usually, keeping the password as a non-expired password is the preferred option.

Broadcom Top Secret user passwords are stored in the Broadcom Top Secret database. You will have to set a temporary password in RACF for all users. The Broadcom Top Secret passwords will need to be retrieved via the Broadcom Top Secret TSSINSTX exit. This exit will need to be modified so that the passwords can be retrieved for each user on the system.

Defining passwords to RACF

Some of the users in Broadcom Top Secret may not have a password as shown in the listing above by USER5. As of RACF 2.4, users with no password can be set as protected user IDs by:

```
ADDUSER userid DFLTGRP(group) ... NOOIDCARD NOPASSWORD
```

You will need to define a password for ALL users. By default, the password will be the same as the default group name. If this is unacceptable, you must issue an `ALTUSER PASSWORD` command similar to the one shown below to provide a password of your choice.

For each user with a password, you can issue the `ALTUSER PASSWORD NOEXPIRE` command from a Systems Level `SPECIAL` user ID to set the password and have it not expire.

```
ALU USER1 PASSWORD(PASSW1) NOEXPIRE
```

Defining password interval

Some users are not required to change their password and some may be required to change their password on a frequency different than the system default. From the listing of the passwords shown above, you can determine the password Interval for each user. Use the PASSWORD INTERVAL command to set the interval for each user. The samples below show how to set an interval of 60 days for a specific user and how to set a user so that they are not required to change their password. Password intervals must be set equal to or less than the system default interval defined in the Systems Options (SETROPTS):

```
PASSWORD USER5 NOINTERVAL
PASSWORD USER3 INTERVAL(30)
```

6.2.8 Other Broadcom Top Secret user ACID parameters

The previous conversion methodologies for fields within the Broadcom Top Secret user ACID are some of the major methodologies one needs to consider for each of the fields in use in the Broadcom Top Secret database. Additional information that is needed from the user ACID records will need a conversion methodology designed to convert those fields and user-defined fields to RACF when applicable.

Statistics and history

The statistics and history of a user's access to the system will be recorded in the RACF database as the user begins using the system. The Statistical and History Information from the Broadcom Top Secret database is not usually carried into the new database. If you want the information in the database, you will need to write code to propagate it since there is no command to set statistics. Alternatively, you can record the information in the copy of the database (or flatfile of the database) that you keep to provide historical data.

User attributes

The user attributes are converted to similar attributes in RACF.

- **AUDIT** - Both products have the ability to AUDIT users of the system and both are called AUDIT. RACF also has options for levels of Auditing in the Systems Options, such as SAUDIT, OPERAUDIT, and LOGOPTIONS.
- **SUSPEND/ASUSPEND** - Both the SUSPEND and ASUSPEND users can be converted as REVOKED users in RACF. To continue ASUSPEND Function, several design considerations will be required.
- **BYPASSING** - Broadcom Top Secret allows bypassing of security checking at granular levels such as NOVOLCHK, NODSNCHK, NORESCHK and NOLCFCHK. z/OS allows bypassing by use of the Program Property Table (PPT) and RACF allows bypassing for some users, such as started task TRUSTED function. Otherwise, access will be checked for resources.
- The way Broadcom Top Secret protects data sets (and all other resources) is sometimes referred to as "protection based on the user". What this means is that, when deciding whether a user can access a certain data set, Broadcom Top Secret starts with the user ACID, and then checks for the appropriate XA DATASET rule.

6.3 Converting data sets

The way RACF protects data sets (and all other resources) is sometimes referred to as "Protection Based On The resource". What this means is that, when deciding whether a user can access a certain data set, RACF starts with the data set profile, and then checks the access list of that profile for an appropriate user ID or group.

This difference can create an issue when trying to convert Broadcom Top Secret data set protection (and other resources) to RACF. The following discussion illustrates the problem.

6.3.1 User-based versus resource-based protection

In Broadcom Top Secret, authorization to access data sets is given to each user by checking through the XA DATASET rules that are assigned specifically to that user (or in PROFILES defined given to the user). For simplicity, the following discussion assumes data sets are given at the user Level.

Consider three Broadcom Top Secret users who have the following XA DATASET rules assigned to them, and what would happen if each of them tried to access SYS1.LINKLIB:

```
USER1 -  XA DATASET = SYS1.
   ACCESS  = UPDATE
USER2 -  XA DATASET = SYS1.LINK
   ACCESS  = UPDATE
USER3 -  XA DATASET = SYS1.LINKLIB
   ACCESS  = READ
```

In Broadcom Top Secret, all three users would have `READ` access to `SYS1.LINKLIB`. USER1 and USER2 would have `UPDATE` access to `SYS1.LINKLIB`. The fact that USER3 has an XA DATASET rule that more closely matches the data set (`SYS1.LINKLIB`) being accessed has no bearing on whether USER1 and USER2 can access `SYS1.LINKLIB`. This is because when Broadcom Top Secret determines whether a user should be given access to a particular data set, it looks only at the XA DATASET rules associated with that particular user. Also, different XA DATASET rules can be used to access the same data set.

To convert the above rules to RACF on a 1-to-1 basis, we would use the following RACF commands:

```
ADDSD  'SYS1.**'
PERMIT 'SYS1.**' ID(USER1) ACCESS(UPDATE)
ADDSD  'SYS1.LINK*.**'
PERMIT 'SYS1.LINK*.**' ID(USER2) ACCESS(UPDATE)
ADDSD  'SYS1.LINKLIB*.**'
PERMIT 'SYS1.LINKLIB*.**' ID(USER3) ACCESS(READ)
```

In order to match the Broadcom Top Secret protection, we have to put `USER1` on the access list of all other profiles that start with SYS1. Also, we have to put `USER2` on the access list of all other profiles that start with SYS1.LINK. To do that, we use the following additional `PERMIT` commands:

```
PERMIT 'SYS1.LINK*.**'     ID(USER1)  ACCESS(UPDATE)
PERMIT 'SYS1.LINKLIB*.**'  ID(USER1)  ACCESS(UPDATE)
PERMIT 'SYS1.LINKLIB*.**'  ID(USER2)  ACCESS(UPDATE)
```

Now `USER1` can access any data set starting with `SYS1.` because he is on the access list of all the data set profiles that start with `SYS1`. Similarly, `USER2` can now access any data set starting with `SYS1.LINK` because he is on the access list of both profiles that start with `SYS1.LINK`.

The process of allowing users access to the correct resources by putting all users on the access list is called undercutting and is similar to the undercutting philosophy used in Broadcom Top Secret.

6.3.2 Data set conversion overview

We start by showing you how to convert a simple Broadcom Top Secret resource rule to the commands necessary to create the corresponding RACF protection.

XA DATASET rule

In Broadcom Top Secret, the data sets a user can access are determined by checking the XA DATASET rules related to that user. These rules are found in the individual user ACID, any profile ACIDs the user has access to, and the ALL record. In Example 6-5, USER1 has three XA DATASET rules in his user ACID:

Example 6-5 XA DATASET rules for User1

```
ACCESSORID = USER1    NAME       = AARON AARDVARK
TYPE       = USER      FACILITY   = CICSPROD
PROFILES   = CICSPRF1  TSOPRF1
.
.
.
XA DATASET = CICS.USER                          OWNER(CICSDIV )
   ACCESS  = UPDATE,CONTROL
XA DATASET = SYS1.                              OWNER(SYS1    )
   ACCESS  = READ
XA DATASET = SYS1.PROCLIB                       OWNER(SYS1    )
   ACCESS  = UPDATE
```

When USER1 attempts to access a data set, the DSNAME of that data set is compared to XA DATASET rules in the user ACID. If all the characters in the XA DATASET rule match the start of the DSNAME in the exact order, then that rule is used to determine what access Level USER1 has to the data set. If more than one XA DATASET rule could apply to the same data set, then the rule with the largest number of matching characters is the one chosen. If no rules apply in the user ACID, then Broadcom Top Secret checks for XA DATASET rules in any profiles the user is associated with, usually in the profile order listed in the user ACID. According to the above rules, USER1 can access any of the following:

- Any data set starting with CICS.USER, with either UPDATE or CONTROL Authority
- Any data set beginning with SYS1., with READ Authority
- Any data set beginning with SYS1.PROCLIB, with UPDATE Authority

Note that in the above example, both the second and third rule could apply when USER1 accesses SYS1.PROCLIB. The third rule is used because it has a larger number of matching characters.

6.3.3 Defining data set protection in RACF

In RACF, to allow USER1 access to the same data sets as in the previous example, you have to first define data set profiles to protect the data sets in question. The ADDSD command is used to create these data set profiles. Typical ADDSD commands look like this:

```
ADDSD 'CICS.USER*.**'    OWNER(CICSDIV) UACC(NONE) GENERIC
ADDSD 'SYS1.**'          OWNER(SYS1   ) UACC(NONE) GENERIC
ADDSD 'SYS1.PROCLIB*.**' OWNER(SYS1   ) UACC(NONE) GENERIC
```

Then you need PERMIT commands to add USER1 to the access list of the profiles protecting those data sets. In addition, you have to specify the access authority (READ, UPDATE) so that it matches what USER1 had in Broadcom Top Secret, as follows:

```
PERMIT 'CICS.USER*.**'     ID(USER1)  ACCESS(CONTROL)
PERMIT 'SYS1.**'           ID(USER1)  ACCESS(READ)
PERMIT 'SYS1.PROCLIB*.**'  ID(USER1)  ACCESS(UPDATE)
```

Note: The use of the generic characters such as ** or *.** at the end of each profile is needed to make the data sets covered by the RACF data set profile consistent with what the XA DATASET rule allowed access to. For consistency, we use these same generic characters whenever we create a RACF profile in this book. For further information on the use of generic characters, refer to the *z/OS Security Server RACF Security Administrator's Guide*, SA23-2289.

6.3.4 Data control groups and the RACF high-level qualifier

RACF expects the high-level qualifier of every data set to be defined as a user ID or group before it allows any data set profiles to be created that use that high-level qualifier. For data sets that do not belong to a defined user, a RACF group must be defined before the data set can be protected. RACF refers to these groups as “data control” groups. If, for example, the high-level qualifier of CICS had not been defined as a group before executing the ADDSD 'CICS.USER*.**' command shown previously, then that ADDSD command would fail. To correct the problem, the following command would have to be executed first:

```
ADDGROUP (CICS) SUPGROUP(CICSDEPT) OWNER(CICSDEPT)
```

RACF also requires the high-level qualifier for every data set to be fully qualified. Where you have defined Broadcom Top Secret data set rules with generic characters or without a trailing period, you will need to convert the rule to fully qualified rules for the actual data sets they are intended to cover. For example:

```
Broadcom Top Secret  RACF Rules Needed

ABC+++.             ABCAAA <==== generic characters if data sets exist

                     ABCBBB

                     ABCCCC

                       etc

XYZ111              XYZ111 <=== no period at the end

                     XYZ1112

                     XYZ11123

                       etc
```

The exception to generics in the high-level qualifier is the Broadcom Top Secret rule in the ACID to indicate the user has ALL access to his own data. This is the default in RACF, so a rule is not needed.

```
XA DATASET = %.
   ACCESS  = ALL
```

If the access is not ALL, exits must be written to restrict user access to their own data.

6.3.5 Data set access

Broadcom Top Secret allows access to resources in several ways:

- Owning the data set
- Giving explicit access by XA DATASET rules in USER or PROFILE ACIDs
- Giving general access by XA DATASET in the ALL record

Standard access

What access Level a user has to a data set in Broadcom Top Secret (such as READ or UPDATE), is determined by checking the ACCESS subparameter that immediately follows the XA DATASET rule. The RACF equivalent to this is the ACCESS subparameter of the PERMIT command. A suggested mapping chart to use when converting access authority in Broadcom Top Secret to RACF is shown in Table 6-5. The list is arranged in order from highest to lowest access authority. Throughout this book, the terms “access” and “access authority” often mean the same thing.

Table 6-5 access level conversion

Broadcom Top Secret	RACF
ALL	ALTER
ALTER	ALTER
SCRATCH	ALTER
CREATE	ALTER
CONTROL	CONTROL
WRITE	UPDATE
UPDATE	UPDATE
READ	READ
FETCH	EXECUTE
NONE	NONE

In Broadcom Top Secret, if more than one value is listed in the ACCESS subparameter, then when converting to RACF, choose the value that is the highest among all the values listed for that data set in Broadcom Top Secret. In the example in “Data set conversion overview” on page 70, USER1 had both UPDATE and CONTROL access authority in Broadcom Top Secret. When converting to RACF, the CONTROL value was chosen because it was the higher of the two values.

Ownership access

You will need to add the owner of the data set to the access list with ALTER access if the data set is owned by an individual. In the following example, USER1 will need to be on the access list for any data set beginning with the high-level qualifier of DEPART1.

```
ACCESSORID = USER1     NAME       = AARON AARDVARK
TYPE       = DCA       SIZE       =      512  BYTES
CREATED    = 03/25/98  LAST MOD   = 07/01/2116:42
LAST USED  = 03/26/98 13:40 CPU(CPU1) FAC(TSO     ) COUNT(00606)
DATASET    = DEPART1.
```

```
XA DATASET = SYS3.LINK
   ACCESS  = READ
```

Universal access

The Universal access (UACC) for a data set is equivalent to the resources in the Broadcom Top Secret ALL record. Generally, the UACC should be NONE and the special access of ID(*) added with the general access. For conversion, list the ALL record and give the access in the record to each resource definition in RACF.

6.3.6 Undercutting considerations

The standard Broadcom Top Secret undercutting of the most specific rule applies in the conversion. Depending on the TSSPARM authorization setting, the considerations differ.

Since RACF will use only the most specific rule defined in the database for any given data set, any user who would have been able to access the data set from his user ACID or any permitted profile ACID will need to be on the RACF access list. The following are examples of the undercutting issue in the authorization scenarios.

AUTH(OVERRIDE,ALLOVER)

This is the most common setting and the default. Consider the following example.

```
PROF1                           PROF2
XA DATASET = SYS1.LINK          XA DATASET = SYS1.LINKLIB
   ACCESS  = READ                  ACCESS  = UPDATE
USER1
PROFILES = PROF1 PROF2
USER2
PROFILES = PROF2 PROF1
```

In Broadcom Top Secret, USER1 would have READ access to SYS1.LINKLIB because PROF1 is first in the list of profiles. USER2 would have UPDATE to SYS1.LINKLIB because PROF2 is first in the list of profiles.

In RACF, when the resources from the profiles were converted, they would have both USER1 and USER2 Connected to group PROF1 and group PROF2. After the correction for the undercutting process discussed above, the access lists would be as follows:

```
SYS1.LINK*.**                     SYS1.LINKLIB.**
    PROF1/READ                        PROF1/READ
                                      PROF2/UPDATE
```

USER 2 would have the same access in both Broadcom Top Secret and RACF. USER1 would be incorrect since he now has UPDATE and previously had READ access. The authorization flow for RACF shown in Figure 3-2 on page 25 shows that any *user* on an access list is used before any functional groups (profiles). Therefore, to resolve that access issue, USER1 would need to be put on the access list as an individual user. Naturally, not only USER1 would be put on the access list individually; ALL users with PROF1 in this order must be added.

To convert, any data sets with similar or partial names must be reviewed to determine that they are not in PROFILE Lists for users so that the above problem is created. If such a situation exists, it should be corrected on the Broadcom Top Secret database or each user affected must be put in the access list for all the affected resources in the PROFILEs.

AUTH(MERGE,ALLOVER)

Using the example below, in Broadcom Top Secret both USER1 and USER2 would have READ access to SYS1.LINKLIB since it is the longest name which matches the requested resource in any of the lists of PROFILES for the user.

```
PROF1                           PROF2
XA DATASET = SYS1.              XA DATASET = SYS1.LINKLIB
   ACCESS  = UPDATE                 ACCESS = READ
USER1
PROFILES = PROF1 PROF2
```

In Broadcom Top Secret, USER1 would have READ access to SYS1.LINKLIB because the access would be found using the longest matching name in all the Merged PROFILEs.

In RACF, when the resources from the profiles were converted, they would have USER1 Connected to group PROF1 and group PROF2. After the correction for the undercutting process discussed above, the access lists would be as follows:

```
SYS1.LINK*.**                     SYS1.LINKLIB.**
    PROF1/UPDATE                      PROF1/UPDATE
                                      PROF2/READ
```

USER1 would be incorrect since he now has UPDATE and previously had READ access. The authorization flow for RACF shown in Figure 3-2 on page 25 shows that any *user* on an access list is used before any functional groups (profiles). Therefore, to resolve that access issue, USER1 would need to be put on the access list as an individual user. Naturally, not only USER1 would be put on the access list individually; ALL users with PROF2 must be added.

To convert, any data sets with similar or partial names must be reviewed to ensure that they are not in PROFILE Lists that can cause the problem described above. If such a situation exists, it should be corrected on the Broadcom Top Secret database or each user affected must be put in the access list for all the affected resources in the PROFILEs.

AUTH(MERGE,ALLMERGE)

This option is closest to the RACF philosophy. However, the situation with this authorization is like the AUTH(MERGE,ALLOVER) except that the ALL record must be considered in the merge process.

6.3.7 Other Broadcom Top Secret to RACF data set migration Issues

This section details data set migration issues not covered previously.

ALL record

There are times in Broadcom Top Secret when a user tries to access a data set, and there is no appropriate XA DATASET rule in either the user ACID or any of the PROFILE ACIDs. The ALL record is used by Broadcom Top Secret for those situations. This record is a list of resource rules (data set and others) similar to a profile, except it is almost always the last place Broadcom Top Secret looks for a resource rule to check against. If an appropriate rule cannot be found in the ALL record, then access to the resource depends on the overall security mode that Broadcom Top Secret is in (WARN, IMPLEMENT, and so on). The functions of the ALL record in Broadcom Top Secret are handled by the UACC (Universal access Authority) in RACF. The UACCs are not stored in one central RACF list, but are defined separately (default access=NONE) for each RACF profile.

ACTION

In Broadcom Top Secret, the WARN Mode is used to let a user access a data set at a higher level than the XA DATASET rule would normally allow, but produce a message, for audit purposes, each time this happens. For any one data set, you can selectively allow some users to be in WARN Mode and others in FAIL Mode by use of the ACTION subparameter. For example:

```
ACCESSORID = USER1
XA DATASET = SYS1.LINKLIB                  OWNER(TECHDIV )
   ACCESS   = READ
   ACTION   = WARN
```

In RACF, the ADDSD WARNING subparameter is used for the same purpose; namely putting a data set in WARN mode; but it applies to all accesses to that data set by everyone, and cannot be given selectively to only certain users. By default RACF rules will be in FAIL or DENY equivalent mode.

FAC

Any XA DATASET rules with the FAC must be evaluated for the access you want the user to have in all conditions. access to data sets is provided to the list of users regardless of the application they are using.

```
XA DATASET = SYS1.LINK
   ACCESS  = READ
   FAC     = TSO
XA DATASET = SYS1.LINK
   ACCESS  = UPDATE
   FAC     = BATCH
```

PRIVPGM and LIBRARY

Both products can control access to data sets through program pathing (Broadcom Top Secret) or program access to data sets - PADS (RACF). Broadcom Top Secret does it through the data set rule by using the LIBRARY and/or PRIVPGM parameters.

RACF uses the PROGRAM class to define the controlled programs and libraries. On the data set profile the additional statement WHEN(PROGRAM(xxx)) results in a conditional access list which is used to restrict access only through this program.

The following must be observed:

- The PROGRAM must be protected.
- The conditional access list must be defined.
- PADCHK or NOPADCHK must be specified.

An example of the Broadcom Top Secret access rule entry is:

```
ACCESSORID = PROF1
XA DATASET = SYS1.PAYROLL
    ACCESS  = UPDATE
    LIBRARY = PROD.LOADLIB
    PRIVPGM = PAYUPDT
```

The example above results in the following RACF commands:

1. Define the program PAYUPDT in library 'PROD.LOADLIB' to the PROGRAM Class (the library must be in the LNKLIST concatenation):

```
   RDEFINE PROGRAM PAYUPDT -
```

```
      ADDMEM('PROD.LOADLIB'//NOPADCHK) UACC(READ)
```

2. Permit group PROF1 (or USER1) to ALTER access to data set 'SYS1.PAYROLL' when executing program PAYUPDT from library 'PROD.LOADLIB':

```
    PERMIT 'SYS1.PAYROLL' ID(PROF1) -
      ACCESS(ALTER) WHEN(PROGRAM(PAYUPDT))
```

UNTIL

In Broadcom Top Secret, the UNTIL parameter lets you create an XA DATASET rule that expires on a specified date. In the following example, USER1 has access to the SYS1.LINKLIB data set with ALL authority Until 12/04/22, at which time the access is revoked:

ACCESSORID = USER1

XA DATASET = SYS1.LINKLIB   UNTIL(12/04/22)

ACCESS   = ALL

These parameters can be converted by implementing the RESUME and REVOKE parameters of the RACF CONNECT command. By creating a holding group for the resource being Protected, Connect the groups matching the UID String to this holding group and specify the RESUME and REVOKE parameters to cover the period indicated by the UNTIL parameters.

```
ADDGROUP (EXPIRE1)
ADDSD   'SYS1.LINKLIB*.**'
PERMIT  'SYS1.LINKLIB*.**'  ID(EXPIRE1)  ACCESS(ALTER)
CONNECT USER1  GROUP(EXPIRE1)  REVOKE(12/04/22)
```

In the above example, USER1 is granted ALTER access to SYS1.LINKLIB because they are connected to the group EXPIRE1. This connection to that group will be revoked on 12/04/22, and with it, their access to SYS1.LINKLIB.

6.3.8 More data set considerations

Some general observations on converting data set rules are provided in the this section.

Discrete versus generic profiles

Broadcom Top Secret TSSPARM has a parameter for ADSP. RACF has the same option in the systems options. In both cases, it indicates that a data set is to have the protect bit set in the DSCB. In RACF, this is called a *discrete data set profile*. Discrete means it covers only this specific data set on this specific volume/unit combination and the DSCB protect flag is set. When such a data set is opened, RACF will search for a discrete profile. If no such profile is found, it will look for a generic profile that could cover the request. To help administration, use generic profiles whenever reasonable. When one generic profile can cover many data sets, this will also improve system performance. However, using too many fully-qualified generic profiles can hurt both performance and administration.

Even if the data set has no generic characters and is fully qualified in Broadcom Top Secret, that is, it has single quotes around the name, it should be generated as a RACF fully qualified generic in most cases. To ensure a data set is generic, include the word GENERIC or the abbreviation G on the ADDSD command.

```
In Broadcom Top Secret
XA DATASET = ‘SYS1.LINKLIB’       OWNER(DEPT1)
   ACCESS  = READ
XA DATASET = SYS1.PARM            OWNER(DEPT1)
```

```
   ACCESS = READ
In RACF
ADDSD SYS1.LINKLIB OWNER(DEPT1) UACC(NONE) GENERIC
ADDSD SYS1.PARM*.** OWNER(DEPT1) UACC(NONE) G
```

> **Note:** Broadcom Top Secret will ignore the DSCB protect bit if it is set and the TSSPARM specifies ADSP(NO). RACF always checks the discrete profiles, DSCB bit on, first. If it is possible that any data sets were created with the DSCB protect bit set, you should run the TSSPROT utility to find and reset the bits before conversion to RACF.

Erase-On-Scratch (EOS)

EOS should be used for confidential data to ensure that residual data cannot be accessed after deletion. Residual data is a potential security exposure for confidential data. In Broadcom Top Secret, EOS is done on a system level, based on the TSSPARM AUTOERASE and MODE options. In RACF it can be done on a data set level and as such, it can be very selective and used without causing performance problems.

6.4 Converting resources

We use the term “resource rules” to indicate the definitions in Broadcom Top Secret that describe what resources any particular ACID is allowed to access. data set resources are covered in the previous section. This section will concentrate on the other resources. Table 6-6 shows the resource rules and their RACF equivalents.

Table 6-6 Resource rules and RACF equivalents

Resource rule	Typical RACF equivalent
FACILITY	CLASS(APPL)
XA OTRAN	CLASS(TCICSTRN/GCICSTRN) or user-defined CICS or IMS Class
XA VOLUME	CLASS(FACILITY) $DASDI
XA ACID	CLASS(SURROGAT)
XA TERMINAL	CLASS(TERMINAL)
XA PROGRAM	CLASS(PROGRAM)
XA IBMGROUP	GROUP
XA user-defined	CLASS(user-defined)

It is important to note that there are many alternatives you can use when converting non-data set protection. The following examples are suggestions of how you can convert your non-data set rules. There is usually no one “right answer” when choosing an algorithm to use to convert each of the resource rules. However, in order to determine the most accurate and appropriate conversion algorithm for each resource rule, you should do the following:

1. Thoroughly understand what that rule protects in the Broadcom Top Secret environment.
2. Determine how RACF accomplishes the same protection.
3. Determine what RACF command is used to create that protection.

You then can create the necessary algorithm to convert that particular resource rule.

6.4.1 FACILITIES

A **FACILITY** in Broadcom Top Secret usually becomes an application in RACF. The **APPL** general resource class is used by RACF to provide this type of protection. There is not always a 1-to-1 correspondence between facilities and applications. Having access to a **FACILITY** in Broadcom Top Secret often allows you access to more than one application. Some applications that are defined as a **FACILITY** in Broadcom Top Secret, such as BATCH and TSO, will not be protected by the **APPL** class in RACF unless there is a product or application that requires it.

A suggested conversion approach is as follows:

1. Identify what you have defined as facilities in your Broadcom Top Secret environment.
2. Document what specific applications are covered by each facility.
3. Determine what the VTAM ACBs are of these applications.
4. Determine other applications you may wish to protect that may not be listed in your Broadcom Top Secret database.
5. Create `RDEF APPL` commands to define the applications to RACF.
6. Create `PERMIT` commands to allow access to the applications.

For example:

```
Broadcom Top Secret FACILITY statements:
ACCESSORID = PROF1
FACILITY   = BATCH      doesn't convert to an APPL in RACF.
FACILITY   = CICSPROD   allows access to CICS1, CICS2, CICS3.
In RACF, may become:
RDEF   APPL  CICS1  UACC(NONE)
RDEF   APPL  CICS2  UACC(NONE)
RDEF   APPL  CICS3  UACC(NONE)
PERMIT CICS1 CLASS(APPL) ID(PROF1) ACCESS(READ)
PERMIT CICS2 CLASS(APPL) ID(PROF1) ACCESS(READ)
PERMIT CICS3 CLASS(APPL) ID(PROF1) ACCESS(READ)
```

6.4.2 Volume

XA VOLUME is a very powerful rule in Broadcom Top Secret. Broadcom Top Secret checks these rules before **XA DATASET** rules. Depending on how these rules are coded, some users may be allowed access to data sets through the **XA VOLUME** rule that they normally would be denied access to through the **XA DATASET** rule. **XA Volume** is another Broadcom Top Secret rule that is set up for security for your storage protection for your DASD volumes. While there is a RACF facility rule that is available that can be used to determine who can allocate space on a volume, this is an obsolete way of handling the conversion of this Broadcom Top Secret rule. A better way is to migrate to IBM's Storage Management Subsystem and/or DFDSS product which can handle the administration of your DASD volumes as well as administer your data put on those volumes. RACF does not have a facility that allows someone access to a data set that they are not authorized to, because of some sort of “override” based on the volume the data set is on. Protection of that type is better handled by DFSMS routines.

You can use the information from these **XA VOLUME** rules to create a very limited type of volume protection in RACF. For example, the **FACILITY** class in RACF can be used to determine who can allocate space on a volume when creating data sets. An appropriate IGGPRE00 exit must be installed as well.

Also, the **DASDVOL** class in RACF can be used to allow someone access to data sets by volume instead of by checking data set profiles. However, access is granted only when the user is performing a DASD maintenance function, such as backing up a pack. Access is not granted if the user is trying to browse or update the file.

For volume protection of **BLP**, RACF has the **FACILITY** class of **ICHBLP** to provide the same function.

```
Broadcom Top Secret listing:
   USER1 -  XA VOLUME = TAPE
               ACCESS = BLP,UPDATE
RACF commands:
   RDEF FACILITY ICHBLP.TAPE UACC(NONE)
   PERMIT ICHBLP.TAPE* CLASS(FACILITY) ID(USER1) ACCESS(UPDATE)
    USER1 can now use Bypass Label processing on volumes starting with TAPE
```

For volume protection of **ALL** or **READ**, a special action, possibly an exit, will be required to preserve the function.

6.4.3 The Online Transaction (OTRAN)

Online transactions require special consideration and planning to translate. Before you create the new online security definitions, you should be very familiar with how RACF protection works with the individual products, particularly with CICS, and what performance issues are involved when defining your transactions to RACF.

For CICS, recommendations include:

- Define your transactions to RACF in a manner that minimizes defining the same transaction to multiple RACF profiles.
- Only permit the transaction profiles to groups, and not to individual users.
- Connect users who have to use the transactions to the appropriate groups.

For example:

Broadcom Top Secret **XA OTRAN** statements:

```
ACCESSORID = PROF1
DEPT ACID  = DPT1
XA OTRAN   = CEMT
XA OTRAN   = DC01
XA OTRAN   = DC02
ACCESSORID = PROF2
DEPT ACID  = DPT2
XA OTRAN   = DC01
XA OTRAN   = DC02
```

In RACF:

```
RDEF   TCICSTRN CEMT UACC(NONE)
RDEF   TCICSTRN DC01 UACC(NONE)
RDEF   TCICSTRN DC02 UACC(NONE)
PERMIT CEMT CLASS(TCICSTRN) ID(PROF1) ACCESS(READ)
PERMIT DC01 CLASS(TCICSTRN) ID(PROF1,PROF2) ACCESS(READ)
PERMIT DC02 CLASS(TCICSTRN) ID(PROF1,PROF2) ACCESS(READ)
```

6.4.4 Limited Command Facility (LCF) AUTH/EXMP

`LCF AUTH` for transactions should be converted the same as described previously for the `OTRAN`. If there is an `OTRAN` and an `LCF AUTH` for the transaction, the `OTRAN` is the one to be converted.

`LCF AUTH` for other than transactions must be evaluated. Often the facility is a TSO command which, if needed, can be converted to program protection for the module which is called for the TSO command. Other facilities will probably require new resource classes and/or exits to control.

`LCF EXMP` commands can add many users to the access list with `ACCESS(NONE)` due to undercutting issues. Remember, each `PROFILE` is a RACF group on the access list and the common way to prevent the group access from being used is to put individuals on the access list. This method will work for transactions and program protection. Other methods may be required for other facilities protected.

6.4.5 Db2

There are three areas in which control of Db2 resources can be protected. These controls can be implemented in both Broadcom Top Secret and RACF, and are:

- Control of access to Db2 subsystems
- Control of access to Db2 secondary authorization IDs
- Control of access to Db2 objects through the use of external security

Access to Db2 subsystems

Controlling access to the Db2 subsystem from different environments (e.g, TSO,BATCH, CICS, or IMS) is accomplished by Db2 issuing a Security Access Facility (SAF) call to see if the user is allowed access to the subsystem by using a specific environment. Since this Db2 control is using SAF, conversion from Broadcom Top Secret is rather straightforward.

In Broadcom Top Secret

```
ACCESSORID = USER1
XA Db2     = DSNR.DBPROD.BATCH
XA Db2     = DSNR.DBPROD.DIST
```

In RACF:

```
RDEF DSNR DBPROD.BATCH UACC(NONE) OWNER(... )
PERMIT DBPROD.BATCH -
 CLASS(DSNR) ID(USER1) ACCESS(READ    )
RDEF DSNR DBPROD.DIST UACC(NONE) OWNER(... )
PERMIT DBPROD.DIST  -
 CLASS(DSNR) ID(USER1) ACCESS(READ    )
```

Secondary authorization

An IBMGROUP in Broadcom Top Secret becomes a group in RACF. Each XA IBMGROUP rule should be defined to RACF by using the `ADDGROUP` command. The subgroup of each IBMGROUP is the owner that is listed next to each XA IBMGROUP rule. The users who have these resource rules in their ACIDs should be connected to the corresponding groups in RACF. For example:

In Broadcom Top Secret

```
ACCESSORID = USER1
XA IBMGROUP= Db2GRP     OWNER(Db2)
```

In RACF:

```
ADDGROUP Db2GRP SUPGROUP(Db2)
CONNECT USER1 Db2GRP
```

Note that DB2GRP might be both a profile ACID and a IBMGROUP. This is allowable in Broadcom Top Secret. However, RACF lets you use DB2GRP as a group or a user, but not as both. If the same name was used as a PROFILE ACID, for example, and a IBMGROUP, two groups with the same name would be created, which is not allowed. The people on the connect list may not need both the secondary group and the functional group. You may have to rename some of the IBMGROUPs or some ACIDs as part of the conversion effort.

Controlling access to Db2 objects

A user can have access to Db2 objects, such as tables and plans. Db2 has it own access control mechanism to control these objects, maintained through Db2 administration. Controls of these objects can also be implemented by using Db2 external security. Broadcom Top Secret has a Broadcom Top Secret subsystem feature to accomplish this; RACF provides this access control through the RACF/Db2 External Security Module (ESM).

Controlling access to Db2 objects using external security and its implementation is different in Broadcom Top Secret and RACF. Some of the Db2 privileges in Broadcom Top Secret's external security subsystem do not directly translate on a one-to-one basis. Conversion and careful attention to this will be needed to ensure these privileges get mapped to the correct RACF classes.

6.4.6 Terminal

XA TERMINAL corresponds to the **TERMINAL** class in RACF. For example:

In Broadcom Top Secret:

```
ACCESSORID = USER1
XA TERMINAL= A11
```

In RACF:

```
RDEF TERMINAL A11 UACC(NONE) OWNER(owner)
PERMIT A11 CLASS(TERMINAL) ID(USER1) ACCESS(READ)
```

USER1 can now access the system through terminal A11. Terminal definitions in RACF are for TCP/IP or LU definitions. An example of how to define this for RACF follows:

1. Define the terminal ID (VTAM LU name or TCP/IP address) as a protected resource to RACF in class TERMINAL.
2. Run the following command.

   ```
   RDEFINE TERMINAL (terminal id) UACC(NONE)
   ```

3. Permit each user that can log on from this terminal (terminal id) by using the following command.

   ```
   PERMIT (terminal id) CLASS(TERMINAL) ID(userid) ACCESS(READ)
   ```

6.4.7 Program

RACF uses the **PROGRAM** class to define controlled programs and libraries. On the data set profile, the additional statement **WHEN(PROGRAM(xxx))** results in a conditional access list which is used to restrict access only through this program.

Program protection requires the following:

- The program must be defined to the **PROGRAM** class.
- In the **PROGRAM** class, both library name and the program name are specified. Optionally, the volume for the library may be specified.
- Any aliases of the program being defined must also be included in the **PROGRAM** class profile.
- In addition, the **PROGRAM** class profile can specify **PADCHK** or **NOPADCHK (PADCHK** is the default). **PADCHK** adds the following additional requirements:
  - All programs represented by the opening task’s PRB must be controlled in a class **PROGRAM**.
  - All programs that link to, load or call the program that opens the data set must be controlled in class **PROGRAM**.
- **PADCHK** may be difficult to establish and maintain and is therefore rarely used.

A **PROGRAM** class definition will look like the example below. Define the program **PAYUPDT** in library 'PROD.LOADLIB' to the **PROGRAM** class.

```
RDEFINE PROGRAM PAYUPDT -
   ADDMEM('PROD.LOADLIB'/volser/NOPADCHK) UACC(READ)
```

6.4.8 XA ACID

XA ACID corresponds to the **SURROGAT** class in RACF. For example:

In Broadcom Top Secret:

```
ACCESSORID = USER1
XA ACID    = USER2
```

In RACF:

```
RDEF SURROGAT USER2.SUBMIT UACC(NONE) OWNER(USER2)
PERMIT USER2.SUBMIT CLASS(SURROGAT) ID(USER1) ACCESS(READ)
```

USER1 can now submit jobs with `USER=USER2`. Typically, XA ACID rules convert in a very straightforward manner.

6.4.9 User-defined resources

If you have created your own resources, either for a purchased product or for an application, then you may have made changes to the **TSSPARM** to use an existing (pre-defined) facility or you have modified the Resource Descriptor Table (RDT) to create your own resource name. RACF has an equivalent function which is the class Descriptor Table (CDT). The CDT contains the names of all known resources classes for RACF. To use your defined resources or those defined to Broadcom Top Secret that are not in the CDT, you must add them to the user portion of the CDT. The access to these resources can be converted using the same methodology as other resources. For example:

In Broadcom Top Secret:

```
ACCESSORID  = USER1
XA MYDEFINE = MYDATA
   ACCESS   = READ
```

In RACF:

```
RDEF MYDEFINE MYDATA UACC(NONE) OWNER(DEPT1)
PERMIT MYDATA CLASS(MYDEFINE) ID(USER1) ACCESS(READ)
```

6.5 Other considerations

This section discusses considerations for other resources not previously covered, such as Unix System Services (USS).

6.5.1 z/OS UNIX considerations

The UNIX group (the RACF group containing the group ID or GID) must be the current connect group for the GID to take effect. With **`LIST`** of **`GROUPS CHECKING`**, most people do not change their group at logon. Therefore, for conversions, change the default group of the users with **`OMVS`** segments to the **`DFLTGRP`** specified in the USER ACID and connect the user to the appropriate department. An example is:

```
ACCESSORID = $USER3      NAME             = AARON AARDVARK
TYPE       = USER        SIZE             = 768  BYTES
DEPT ACID  = DEPT1       DEPARTMENT       = DEPARTMENT ONE
DIV ACID   = DIV1        DIVISION         = DIVISION ONE
CREATED    = 11/11/99    LAST MOD         = 24/03/21 12:34
PROFILES   = PROF1    PROF7
GROUPS     = OMVSGRP
LAST USED  = 25/03/00 13:26 CPU(CPU1) FAC(TSO     ) COUNT(00645)
DFLTGRP    = OMVSGRP
MYDEFINE   = MYDATA
----------  SEGMENT OMVS
HOME       = /
OMVSPGM    = /bin/sh
UID        = 0000009303
```

This would have been:

```
ADDUSER $USER3 DFLTGRP(DEPT1) OMVS(...
```

It will now change to:

```
ADDUSER $USER3 DFLTGRP(OMVSGRP) OWNER(OVMSGRP) OMVS(...
CO $USER3 GROUP(DEPT1) OWNER(DEPT1)
```

If the user is created by an automated process with all users, the user would only need the following commands to change the default group:

```
CO $USER3 GROUP(OMVSGRP) OWNER(OMVSGRP)
ALTUSER $USER3 DFLTGRP(OVMSGRP)
```

6.5.2 Started tasks (STC)

This section describes the conversion of started task authorization.

To get the currently defined procedures and users associated with them, you would simply list them as shown below.

In Broadcom Top Secret

```
TSS LIST(STC)
Output
 ACCESSORID = *STC*     NAME       = STARTED-TASKS
                        SIZE       =     2816  BYTES
 CREATED    = 04/03/00  LAST MOD   = 07/20/21 15:43
 STC        = *DEF*     ACID       = *BYPASS*
 STC        = APPC      ACID       = APPCTP
 STC        = ASCH      ACID       = APPCSCH
 STC        = ASCHINIT  ACID       = APPCINT
 STC        = BPXAS     ACID       = OMVS
 STC        = BPXOINIT  ACID       = OMVS
 STC        = CICSTEST  ACID       = CICSTST
 STC        = CICSPRDA  ACID       = CICSPRA
 STC        = CICSPRDB  ACID       = CICSPRB
 STC        = CICSPRDC  ACID       = CICSPRB
 STC        = DSNDBM1   ACID       = Db2DBM1
 STC        = DSNMSTR   ACID       = Db2MSTR
 STC        = OMVS      ACID       = OMVS
 STC        = RMFGAT    ACID       = RMFGAT
 STC        = SPECIAL   ACID       = *BYPASS*
 STC        = TCPIP     ACID       = TCPIP
 STC        = VTAM      ACID       = NET
```

Note that there are some **PROCs** that use the same user ID as another PROC and there are some that are unique to the **PROC**. This is the same as in RACF. There may be more started tasks required in RACF than are currently defined in Broadcom Top Secret because RACF is started sooner in the IPL process than Broadcom Top Secret and can, therefore, protect more system functions.

RACF has two methods to support started tasks: Started Class and Started Table. The recommended method is the started class. In both cases, RACF uses a class or table to associate a user ID and group name with a started procedure. Normal access checking is performed for all started procedures using the associated RACF user ID and group dame defined. It is very important to have the *user* and *group* definitions match in the class or table. If they do not, the entry will not be used and the default or undefined user will be used for the started task.

You can indicate that selected started procedures are to be considered as **TRUSTED** similar to the **BYPASS** option in Broadcom Top Secret. **TRUSTED** will allow access to data sets without the user being on the access List.

The class or table may include a generic entry similar to the *DEF* entry in the sample above. The generic entry will apply to all started tasks not defined in the class or table. A sample class entry and a sample table entry are:

Sample STC class entries

```
RDEF STARTED CICSPRDA.* OWNER(xxxx)
     STDATA(USER(CICSPRDA) GROUP(STCGROUP) TRUSTED(NO)
RDEF STARTED *.* OWNER(xxxx)
     STDATA(USER(=MEMBER) GROUP(STCGROUP) TRUSTED(YES)
Sample STC Table entries
DC   CL8'CICSPRDA'               STARTED PROC NAME
DC   CL8'CICSPRDA'               ASSIGNED USER
DC   CL8'STCGROUP'               ASSIGNED GROUP
DC   XL8'0000000000000000'       ATTRIBUTES
DC   CL8'*       '               STARTED PROC NAME
DC   CL8'=       '               ASSIGNED USER
DC   CL8'STCGROUP'               ASSIGNED GROUP
DC   XL8'0400000000000000'       ATTRIBUTES
```

Refer to *z/OS RACF System Programmer's Guide,* SA23-2287 for a more detailed description.

6.6 Converting system-wide options

This section describes some of the system-wide security options for both Broadcom Top Secret and RACF. These options determine how the security product is protecting your system. A table is included to show the most direct mapping of some of the Broadcom Top Secret global system options to RACF's system-wide options.

6.6.1 Common system-wide security options

Table 6-7 contains the system-wide options common to both Broadcom Top Secret and RACF.

Table 6-7 System-wide options common to Broadcom Top Secret and RACF

Broadcom Top Secret	RACF
ADSP	ADSP/NOADSP[a]
AUTH(xxx,yyy)	GRPLIST
AUTOERASE(NO)	ERASE/NOERASE
MODE(...)	PROTECTALL(...)/NOPROTECTALL
HPBPW(n)	JES(EARLYVERIFY)) - required default
INACTIVE(nn)	INACTIVE(nn)
NEWPW	PASSWORD(...)[b]
PWEXP(nn)	PASSWORD(INTERVAL(nn))
TAPE	TAPEDSN/NOTAPEDSN
TEMPDS(NO)	TEMPDS

[a] Be sure to review "Discrete versus generic profiles" on page 76.
[b] See PASSWORD options in Appendix B.4.1, "Passwords" on page 103.

6.6.2 The Command Propagation Facility (CPF)

The Command Propagation Facility (CPF) includes several statements in the **TSSPARM** such as **CPFNODES, CPFRCVUND, CPFTARGET,** and **CPFWAIT**. RACF also can propagate changes across systems using the RACF Remote Sharing Facility (RRSF).

6.6.3 Protection modes

Both products can be set to enforce default data set protection, that is, denial of access to data sets not covered by a Broadcom Top Secret definition or a RACF profile. When no Broadcom Top Secret rule is found for a data set, the **TSSPARM MODE** option will decide what will happen. If **MODE** is set to **FAIL**, the data set must have a matching rule set, otherwise access is denied. If the global RACF option **PROTECTALL(FAILURES)** is set, RACF will require a matching profile for all accessed data sets. Without a profile match, access will be denied, so Broadcom Top Secret’s **MODE=FAIL** and RACF’s **PROTECTALL(FAILURES)** will both require all data sets to be protected.

Passwords

Many of the password rules can be converted. Listed are some of the RACF options. The **PASSWORD** parameter of Systems Options specifies the monitoring and checking of passwords by indicating the following sub-operands.

HISTORY() Specifies that 1 to 32 previous passwords are saved and compared to a new password if specified.

INTERVAL() Indicates the number of days that the current password is valid (1 to 254). This value is used as a default for new users added with the `ADDUSER` command and is also used as the upper limit for the `INTERVAL` operand of the `PASSWORD` command.

REVOKE() Indicates the number of invalid passwords that can be entered before RACF revokes the user ID.

RULEn() Specifies one to eight individual password syntax rules. The rule contains a length attribute and content keywords describing valid passwords. For example:

```
RULE1(LENGTH(8) ALPHA(1:3) CONSONANT(4,8) NUMERIC(5:7))
```

You can use the ICHPWX01 exit to perform additional checks for password rules, such as, the password cannot be equal to the user ID.

6.6.4 RACF options

This section describes some additional RACF options that are highly recommended when defining system-wide protection for your installation. The following example specifies that all the current RACF options be displayed.

```
SETROPTS LIST
```

Additional RACF `SETROPTS` parameters can include:

NOADDCREATOR specifies that if a user defines any new data set or general resource profile, RACF does not place the profile creator's user ID on the profile's access.

EGN activates enhanced generic naming (EGN). This option allows you to specify the generic character ** (in addition to the generic characters asterisks(*) and percent(%)).

GENCMD(*) activates generic profile command processing for all classes and needs to be reissued each time a new class is added.

GENERIC(*) activates generic profile checking for all classes except grouping classes and needs to be reissued each time a new class is added.

GRPLIST specifies that authorization check processing is to perform list-of-groups access checking for all system users. When you specify `GRPLIST`, a user's authority to access or define a resource is not based only on the authority of the user's current-connect group; access is based on the authority of any group of which the user is a member.

JES(BATCHALLRACF) specifies that JES is to test for the presence of a user ID and password on the job statement or for propagated RACF identification information for all batch jobs. If the test fails, JES is to fail the job.

PREFIX() Enables protection of data sets with a single-qualifier data-set name and specifies an HLQ to be prefixed to these data-set names during RACF authorization processing. The prefix should be a defined group name and not an existing HLQ.

PROTECTALL() Enables protect-all processing. All data sets that do not have a RACF profile cannot be accessed, including data sets on DASD, GDG, and catalogs. Tape data sets are also included if `TAPEDSN` is active. **NOPROTECTALL** specifies that a user can create or access a data set that is not protected by a profile.

The two operands used with **PROTECTALL** are:

- **FAILURES** - Causes RACF to deny access to all data sets that are not protected with a RACF profile.
- **WARNING** – Causes RACF to allow access to data sets that are not protected by a RACF profile and issue a warning to the user and security administrator. This option should be used during initial conversion testing to assist in setting up data set security protection.

The **PROTECTALL** parameter pertains only to data set protection. General resources are covered only by their existing Resource profiles with specified Access Levels and an optional **WARNING** parameter. Note that default protection of General resources can be controlled by “catch-all” profiles, such as a profile definition of ‘*’ with **UACC=NONE**.

For more detailed information on RACF’s system-wide options refer to the *z/OS Security Server RACF Command Language Reference*, SA23-2287.

7

Administration and maintenance

The administration of the security subsystem is an important factor when selecting the subsystem, or when migrating to another one. In general, normal z/OS users see only the effects of the security system, and very seldom issue commands directly to it. security administrators, however, frequently issue commands to the security subsystem, and the structure (and convenience) of this process is important to them.

7.1 The administrative interface

RACF administration consists of several different categories of tasks:

1. Routine, day-to-day functions, such as adding users, resetting passwords, adding resource protection profiles, and so forth.
2. Higher-level administration, such as adding new **SPECIAL, GROUP SPECIAL**, **Users**, setting **AUDIT** controls, and so forth.
3. Setting global RACF controls.
4. Maintaining the database, in the sense of purging unwanted entries, detecting unwanted situations, monitoring the correctness of the security policy reflected by the database, and so forth.
5. Monitoring the audit records written by RACF.
6. Maintaining the database, in the sense of backups and reorganization, monitoring performance, and so forth.

RACF commands are normally used for the first three tasks in this list. There are a number of ways to enter RACF commands, and these are discussed in the following sections.

There are many ways to address the fourth task, database quality maintenance. The use of the RACF **SEARCH** command or the **IRRRID00** utility is a starting point and may be all that is required. In more demanding cases, you might need to write or obtain an application to address this area.

The fifth task, monitoring audit records, involves listing selected SMF records. The RACF report writer (no longer actively maintained by IBM) is an easy starting point. There are many SMF reporting programs, including the SMF unload utility that is part of RACF, which can be used with Db2 or DFSORT’s **ICETOOL**.

The sixth task, physical care of the database, involves several utilities supplied with RACF, and also involves normal z/OS tuning activities.

7.2 Commands

Broadcom Top Secret and RACF both have their own command sets. In each case, ISPF panels are available to ease the use of the commands, but the underlying line commands are central to understanding the use of the product. Both products have extensive documentation. Refer to *z/OS security Server RACF Command Language Reference*, SA23-2292, for an explanation of all RACF commands and syntax.

- RACF commands may be entered in a number of ways:
- RACF commands from the TSO command line
- ISPF panels (provided with RACF)
- Batch jobs (which issue the same commands as under TSO)
- Application programs (or third-party products) that issue RACF commands
- RACF commands from z/OS operator consoles

Most commonly, TSO line commands and the ISPF panels are used for day-to-day administration and batch jobs are useful for bulk updates.

RACF commands issued from a z/OS operator's console are very useful in critical situations, but are not intended for routine administration. The operator must have performed a logon function (password authentication) before entering RACF commands. (An exception exists for the operator command that switches to the backup RACF database; an operator logon is not needed in order to issue this command.)

Both products have many commands, and many of these are used only by the security administrator or systems programmers. Only a small part of the full command sets is used daily by other administrators, help desk personnel, and end users.

RACF has four general types of database entities (profiles): User, Group, Dataset, and General Resources. Each of these types has associated commands to add, modify, delete, and list profiles. Table 7-1 lists the basic commands for these operations. The table shows, for example, that the **ALTGROUP** command would be used to alter a group profile.

Table 7-1 RACF commands to ADD, MDIFY, DELETE and LIST resources

	User	Group	Dataset	General resource
Add	ADDUSER	ADDGROUP	ADDSD	RDEFINE
Modify	ALTUSER	ALTGROUP	ALTDSD	RALTER
Delete	DELUSER	DELGROUP	DELDSD	RDELETE
List	LISTUSER	LISTGRP	LISTDSD	RLIST

This table is quite simplistic and is not intended to convey any of the ramifications of the indicated functions. More detailed information on the functionality of the RACF commands can be found in Chapter 3, "IBM z/OS Security Server RACF overview" on page 21. For complete definitions and the syntax of the commands, refer to *z/OS security Server RACF Command Language Reference,* SA23-2292-30*.*

The various privilege levels of RACF commands are described in detail in previous chapters. A very brief summary, related to the use of RACF commands, may be helpful here:

- Someone with the **SPECIAL** privilege can issue any RACF command, except those restricted to auditors. (A **SPECIAL** user can grant himself the **AUDITOR** privilege, and then issue those commands.) This level is usually restricted to a few security administrators. The **SPECIAL** User typically issues global RACF Commands, constructs important generic data set profiles, defines groups, and delegates **Group-SPECIAL** authority.
- Someone with a **Group-SPECIAL** privilege can issue RACF commands that affect only a designated group, or its subgroups. A group may own many subgroups, providing many ways to structure and delegate authority. Distributed security administrators typically have **Group-SPECIAL** Authority for their areas. Help desk personnel may have **Group-SPECIAL** authority.
- The owner of a profile can issue several RACF commands that affect only that profile. In practice, this means that the owner of a data set profile can control which users (and at what level) can access data sets protected by that profile. The primary command involved is **PERMIT**.

In the **PROTECTALL** environment, a RACF profile will already exist for a user's HLQ (created when the user ID was added to RACF). A user can grant permission to other users to access his files. The **PERMIT** command is used for this, and this may be the only RACF command that typical users issue. In a well-designed environment, with appropriate use of generic data set profiles, most users will never need to issue **PERMIT** commands.

RACF commands can be issued from z/OS operator consoles. This should not be regarded as a routine interface for RACF administration, but it can be very useful in an emergency situation. A profile class, `OPERCMDS`, is used to control which operators can issue which RACF commands. Operators are required to log onto the z/OS operator console before they can issue RACF commands.

Once the basic command structure is understood, using RACF commands instead of Broadcom Top Secret commands should not present any problems. The more important migration issues are the organizational processes that occur before any commands are issued.

In practice, Broadcom Top Secret and RACF commands are usually issued from the TSO command line (more experienced administrators) or from ISPF panels. In both cases, a good understanding of the security policy in use and the use of consistent naming conventions and Group conventions, is key to understanding and using the security administrative commands. In both cases, commands can be batched by using the `PGM=IKJEFT01` method of running TSO functions in batch jobs.

7.3 RACF utilities

Several utilities are provided with RACF. These are normally used in batch jobs and address some of the tasks previously listed. These utilities are:

IRRUT100 This program reads the RACF database, and can search for specified entries. While reading, it checks the correctness of internal index records and other pointers.

IRRUT200 This program will simply copy the RACF database, checking major structural items as it copies. However, it observes all RACF Interlocks for update activities that occur while the copy is in progress. This ensures a logically consistent copy. `IEBGENER` can be used to copy a RACF database, but it does not observe such Interlocks and, if there are RACF updates during the copy, it may not produce a complete copy.

IRRUT400 This program also copies the RACF database, but it reorganizes it at the same time. It can split the database into multiple data sets (for performance) or merging multiple data sets back into one. `IRRUT400` can rebuild internal index records, and generally corrects small structural errors.

IRRADU00 This program unloads the security relevant SMF Records into sequential records. It is readable by a person and can be used as input to external programs.

IRRDBU00 This program unloads the RACF database into sequential records with fields specified in EBCDIC characters. It is readable by a person and can be used as input to external programs. For example, some installations load this data into Db2 and perform “what if” searches there.

IRRRID00 This program searches an unloaded RACF database for user IDs and groups that are about to be removed from the installation. You can specify the user ID or group that will replace these departing user IDs and groups.

7.4 Security reports

Reports are important for security administration, in order to enable tracking and monitoring of events and status of the security environment established, and to uncover changes that could lower or change the expected security level. The problem is to collect and get the correct data to meet the objectives. Too many organizations collect too much data, without having any plan or strategy for its use.

There are two levels of reporting for z/OS security subsystems. One level reflects the contents of the security database and describes what is protected and how it is protected. This is called *status monitoring*. The other level reflects the security events that occurred during a particular period; for example, which users logged onto the system, or what attempted security violations were detected. This is called *event monitoring*.

For both Broadcom Top Secret and RACF, event monitoring is centered around SMF records. There are many programs and products available for listing SMF records.

The usefulness of event monitoring depends on what is monitored; that is, what causes an SMF record to be written? Broadcom Top Secret and RACF have options to control which events cause an SMF record to be written. RACF has an orderly structure of auditing controls for this purpose. Controls exist at both individual profile levels and at the global Level. Since a profile can be used to protect a single data set, or to protect a large number of data sets (with similar high-level qualifiers), auditing controls can be selective.

RACF controls can be set to write SMF records on either access failures (where data set access was prevented by RACF), or on access successes (where data set access was permitted by RACF). In general, reporting of successful accesses is not desired, partly because the volume of SMF records would be too large. However, successful access reporting may be appropriate for a carefully selected set of application data sets. access failure events are typically used to create an SMF record, and a basic part of the security administrator's duties is to review these records.[1]

RACF can also log (to SMF) changes to the RACF database itself, and records are created indicating changes to user profiles with any of the high-level authorities, such as **SPECIAL**, should always be reviewed. Some of the key global controls of RACF, related to auditing, are:

- **SAUDIT** is used to log all commands that need a **SPECIAL** User Privilege. This is used to review activities by these privileged users. It can also be used to recreate profiles and commands from SMF data in an emergency.
- **OPERAUDIT** is used to log all data accesses a user with the **OPERATIONS** privilege is granted, due to this privilege. Access through normal access rights are not logged.
- Use both **SAUDIT** and **OPERAUDIT** to enable auditing of privileged users and their activities.
- **CMDVIOL** is used to switch ON/OFF RACF command reporting; **CMDVIOL** will record all attempts to use RACF commands outside a user's authority.
- **LOGOPTIONS** are used to specify logging options for different resource classes, from no logging to full logging. These can be used to globally force logging of resources in one class to avoid having to specify the **AUDIT** option on each profile.
- **GLOBALAUDIT** can be specified by someone with the **AUDITOR** privilege. This generates audit data without requiring that specific profiles be selected for auditing.

[1] There are many different approaches to this. Some installations want to review every access failure, while others check only for substantial patterns of access failures. An access failure is not a security failure; it is simply an indication that the security subsystem was doing its job. In practice, reviewing every access failure tends to be impractical.

In addition to these global and class options, each resource profile can have its own audit requirements defined through the AUDIT option, from no logging to full logging. This setting will not lower the logging requirement set by the LOGOPTIONS value for that class. All profiles have a default AUDIT setting; for example, for data sets it is AUDIT(FAILURES).

In addition to the various logging options mentioned here, all invalid password attempts are logged by default.

UAUDIT can be set on a user profile to cause all RACF activity for that particular user to be logged. It is an effective way to trace all activities of a user, but must be used with some restraint to avoid writing too many SMF records.

Status monitor involves listing control settings in the security database, and monitoring changes to these controls. SMF records, written by RACF, are useful for detecting changes, while static information must be extracted from the database itself. Several tools are provided by RACF:

- DSMON (Data security Monitor) is a program for reporting on several security settings, user privileges and protection status of important system data sets. It should be run regularly to monitor any changes to any of these security areas.
- The RACF ISPF panels offer a number of options to display various control settings.
- RACFRW (RACF Report Writer) is an ad hoc reporting program. The report writer has been stabilized, so new functions will not be reported. The traditional RACF functions such as data set and resource violations can be reported.
- The IRRDBU00, the RACF database unload utility, produces a sequential file which can be used in a number of ways: viewed directly or through the use of locally-written programs, by loading it into Db2 and executing searches there, or by using any standard report-writing software.
- The IRRADU00 the RACF SMF data unload utility, produces a sequential file of security-related audit data which can be used in a number of ways: you can view the file directly or through the use of locally-written programs, by loading it into Db2 and executing searches there or by using any standard report writing software.
- The RACFICE reporting tool utilizes the ICETOOL function of DFSORT to produce various reports using the output of IRRDBU00 or IRRADU00 or both.

In summary, log and audit functions are an important part of an organization’s security policy. The security policy should clearly define what is expected for logging and audit and how it will be used. This requires some skill and experience, since a balance is needed between what is practical, the effects on performance, the problems of generating too much data, and so forth.

7.5 Availability considerations

Broadcom Top Secret and RACF, when fully implemented and used, are both functions critical to a z/OS production environment. Their availability and recoverability must therefore be carefully designed, planned and tested. Due to different technical features and capabilities of the two products, recovery techniques and strategies differ. Approaches to RACF recovery are discussed in the following sections. In this section, we discuss backup options and provide Figure 7-1 to show the backup data sets.

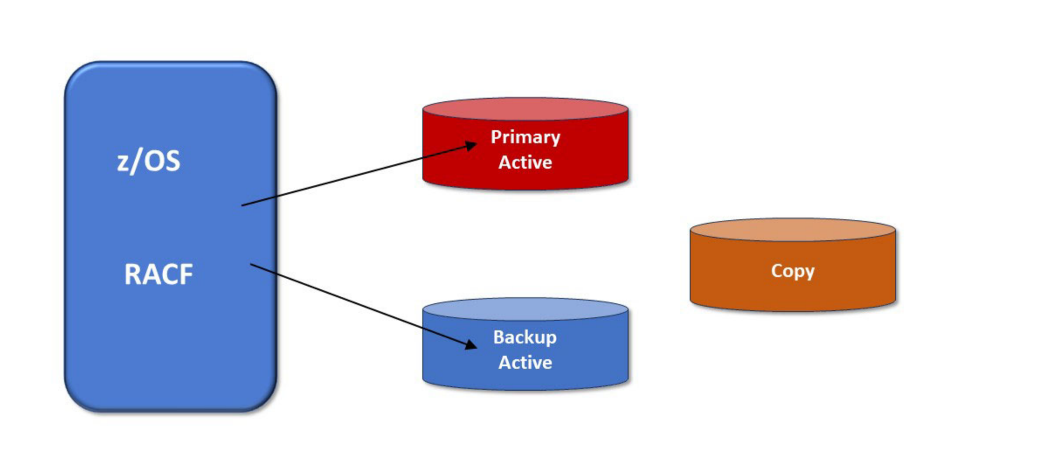


Figure 7-1 RACF primary and backup data sets

7.5.1 RACF active backup option

A unique recovery feature in RACF is the active backup data set option, the commonly used option to maintain a software mirror image of the primary RACF database.

While RACF performs all authentication and authorization checking against its primary database, all updates are automatically duplicated onto the active backup database. In case the primary database is lost, a switch to the backup database can be performed without the need for an IPL or other recovery procedures.

RACF database backup

The initial setup of the RACF recovery environment requires defining the name of the backup data set in the RACF dataset name table, **ICHRDSNT** and making a copy of the primary database (while no updates are taking place). Good recovery strategies also have provisions to periodically take additional backup copies (independent of the active backup). We believe that the best tool to create such copies is the RACF verify utility program **IRRUT200**; this program enqueues on the input database for the duration of the copy process and has the additional advantage that it provides an analysis of the database structure. The **IRRUT200** list output can be used to determine the degree to which the database is full and to identify potential structural problems that need to be addressed.

RACF database recovery

When a problem with the primary RACF database is discovered, an **RVARY SWITCH** command is issued on the system console or in a TSO session to initiate a switch to the active backup database. This one now becomes the primary database and the original primary is deactivated. The system continues to run with just a primary database, and the creation and activation of a new backup database is scheduled for a period of low activity.

To avoid false alarms, this switching capability is secured by a password under the control of the central security administration; this feature can be used to enforce procedures that require the involvement of security management in any RACF status change.

7.5.2 Reorganizing the RACF database

Some organizations include periodic reorganizations of their RACF databases in their backup and recovery plans. In a quiesced environment, use the RACF split/merge utility IRRUT400 to create a “logical” copy of your RACF database (specify one input and one output file). This process eliminates control interval (CI) like splits in the database structure and profiles that have been logically deleted (no pointers in the index structure), but may physically still be present.

7.6 RACF performance considerations

There can be a conflict between your ideal security policy and the performance practicalities of the security subsystem. Controlling CICS transaction accesses is an example of a function that can be torn between security needs and performance needs. Extracting the best performance from the security subsystem involves these areas:

- Using global options that short-circuit the rest of the security monitor.
- Using some type of cache in main storage.
- Using special coding options in applications that result in an unusually fast response by the security subsystem.
- Using a good design for sharing the database file among multiple systems, since the need for a shared security database is common.
- Using normal DASD tuning techniques to improve I/O response.

Both Broadcom Top Secret and RACF provide options in all these categories. Some of these are not simply performance options; they affect the policy design of the security database and should be considered part of your high-level design.

Some of the key RACF features in this area include:

- Global Authorization Check (GAC) - RACF uses this in-storage table to make quick decisions about whether further RACF checking is needed.
- RACLIST refers to the process of moving a complete RACF CLASS of profiles into storage, for faster access.
- In-storage buffers refer to the allocation, in main storage, of a given number of buffers that are managed by RACF with a type of least recently used (LRU) purging technique.
- RACF can take advantage of the coupling facility to further improve performance

If not deflected by a trusted or privileged property, RACF checks the GAC when beginning to process an access request. The GAC is an in-storage table owned by RACF. It is copied into storage when RACF is started, and is static during operation, unless updated by a security administrator. It is usually a very small table. The most typical use is to grant permission to access (in any manner) a data set with the same HLQ as the caller. That is, a user can work with his own data sets (as identified by a matching HLQ) without any further checking by RACF. The GAC can contain lists of exceptions to the General Rules it sets, causing the normal profiles to be checked for these exceptions.

This process can provide excellent performance. The exposure is that no other RACF controls are checked. If, for example, the GAC gives all users READ access to all SYS1 data sets, then no SYS1 data sets can have a general access level of NONE because the profiles that try to establish this condition are not checked. The use of a GAC entry bypassed them. The use of the GAC table is important for performance, but the usage must flow from the overall security policy being defined.

The installation can specify a certain amount of buffer space to be dedicated to a RACF cache, known as *in-storage buffers*. This space is in protected common storage. It is pagable, but for practical purposes can be regarded as fixed because it is referenced frequently. The use of this cache is transparent to policy design, and is a pure tuning function. The cache is limited to RACF elements that are normally read-only, or write-through cache data. The RACF database, on disk, must always reflect current data to other z/OS systems sharing the same database.)

RACF can manage a *backup* database, in addition to its primary database. Practically every installation elects to have a backup RACF database. We do not consider deleting this to be a reasonable action. In addition to profile updates, RACF writes statistical data in its database, for example, the Date and Time of a Users most recent TSO Logon. There is an option to bypass updating the backup database with statistical data. Many installations select this option. In the rare event of a database failure, requiring use of the backup RACF database, some statistical data will be missing. This is usually considered a reasonable tradeoff.

Customers can make use of z/OS's virtual lookaside facility (VLF) to cache accessor environment elements (ACEEs) and information for z/OS UNIX. If RACF finds information in VLF, it will avoid I/O to the database.

The IRRUT400 Utility, supplied with RACF, can be used to reorganize the database. Database performance may degrade slightly over time as updates and changes occur. The effect is usually fairly minor, unless very large databases are involved or many profiles have been added and deleted. A typical installation might use this utility to reorganize the database every six months.

7.6.1 Performance Of shared databases

Sharing a database between Broadcom Top Secret or RACF, among multiple z/OS images has become common. This has a number of interesting effects on performance design, including:

- The use of cache functions becomes more restricted, since the corresponding disk record could be updated by another system, making the cached data invalid.
- Extensive use of RESERVE and RELEASE functions (disk locking commands) can badly impact the performance of a shared disk.
- The use of a disk API (access method) that is not optimized for shared system usage can badly impact performance.

The RACF use of cache (in-storage buffers) is based on a design that avoids cache coherency problems in the presence of shared-system operation.

The elements of RACF operation that affect shared-system performance are all automatic. There is no user tuning involved. The tuning items discussed are effective in both single-system and multi-system environments.

The coupling facility allows z/OS and other software to share data concurrently among multiple systems in the sysplex with the goal of maintaining a single system image. A sysplex with a coupling facility significantly changes the way systems can share data. *Data sharing* is the ability of concurrent subsystems or application programs to directly access and change the same data, while maintaining system integrity. RACF can take advantage of the coupling facility in the sysplex to provide security for the resources of all systems in a comprehensive and centralized way. RACF allows you to use the coupling facility and shared RACF data to help manage the security of resources for all systems in a sysplex.

7.6.2 Migration issues

The complete PPT (program propagation table) should be reviewed manually, as part of any migration effort. Other performance elements, especially the GAC, should be created manually.

Performance elements that do not interact with policy design, such as in-storage buffers and database splitting, can be managed independently from the migration process itself. If the basic migration process, normally through the use of specialized software tools, provides acceptable performance, then it may be advisable to postpone tuning these elements until the end of the migration project.

A CICS installation would certainly want to enable **FASTAUTH** checking for its own applications or program products as part of the migration. This should provide a substantial performance improvement, as well as integrate CICS usage into normal RACF operation.

7.6.3 Summary

Tuning can make a major difference in security subsystem performance. RACF offers a number of major tuning options. Some of these interact with the security policy goals of the system, and this aspect must be considered in the overall design of the RACF implementation. With reasonable designs, RACF can offer significant performance improvements, especially for key areas such as CICS.

A

A Sample migration plan

A migration plan should include the following items. The durations listed are representative, and may vary widely, depending on circumstances.

- Project team education

  While this depends on the availability of classes, once classes become available, about three weeks are needed for attendance. There is little point in attempting to make a detailed project plan (the next step) until key team members have received the necessary education.

- Detailed project planning

  This may take up to two weeks. One of the results should be specific team assignments and schedule targets. This activity requires knowledge of RACF (the existing security manager), the routine operational activities of the installation (including help desk functions, auditing, routine user administration, and so forth), and major production jobs.

- Planning RACF groups

  This activity can easily take several weeks. This activity is the key to obtaining a RACF structure that is manageable, well-designed, and one that meets your needs. This area is where experience (from other RACF migrations) is most important.

- Create a test environment

  This activity can parallel some of the other planning activity, and can take several weeks. In general, it means cloning an existing z/OS, including all the subsystems, and providing access (for testing) to appropriate production files.

- Database conversion

  This can take up to a month. It typically involves using a tool to convert Broadcom Top Secret Database entries to appropriate RACF entries. In practice, the conversion may be done many times by changing the Broadcom TSS input or changing the tool's parameters until the resulting RACF structure meets your design.

  This activity is likely to be intermixed with unit testing and integration testing. After testing a number of your production applications, you may decide a slightly different RACF design would be better; you might then change the conversion tool's parameters and convert your Broadcom Top Secret again.

- Unit testing

Some effort is needed to test your important applications, and contain the testing effort within a reasonable schedule; two to four weeks might be a reasonable target. This phase may require considerable assistance from application owners and production controllers.

- Function testing

  This activity typically takes two weeks. It involves moving several selected applications/users to the test system for production work, and closely monitoring potential problems.

- Production cutover

  This activity involves the final conversion of the Broadcom Top Secret Database to RACF. This phase should include at least three weeks of monitoring and support, to address specific situations that may arise. After this, the migration team could be released.

B

Security policy considerations

Various aspects of security policies have been addressed throughout this document in the context of specific technical discussions. This appendix is intended to consistently summarize policy implementation and enforcement in RACF

We address general policies such as complete RACF control over Users and Resources, naming conventions and resource ownership; we also include discussions of effective and efficient security administration policies and RACF resource utilization.

We do not address mandatory access control policies because we have not observed implementations of these policies in commercial environments.

B.1 User identification

The recommended policy requires that, except for an initial migration, all users must be identified and verified by RACF; in other words, undefined users are not permitted. RACF principally allows for undefined users for two reasons:

- To support an initial migration to a secured environment, and
- To ensure uninterrupted system availability

Techniques to prohibit undefined user IDs vary with the processing environments, as outlined in the following sections.

B.1.1 Batch

SETROPTS BATCHALLRACF is a Global RACF option that enforces the requirements for all batch jobs to have a valid RACF user ID, either through coding USER=user ID on the job statement or through propagation (inheritance).

B.1.2 TSO

To prohibit undefined TSO users, all user IDs defined in SYS1.UADS must also be defined to RACF. The recommended implementation is to use RACF TSO segments for all TSO Users and to keep only a few emergency user IDs in SYS1.UADS. In any case, procedures must be implemented to ensure that the RACF database and whatever entries remain in SYS1.UADS are synchronized, and that user IDs deleted from RACF are also removed from the SYS1.UADS data set.

B.1.3 Started procedures

Started procedures are considered part of the computing environment that is essential to the availability and functionality of the z/OS system. IBM has therefore implemented RACF STC support with focus on availability, for example, with the goal of allowing rather than disrupting the start of procedures. Procedures will start with an undefined user ID under the following conditions:

- The STC user ID (either assigned specifically or through the generic entry in the STC table) is not a RACF-defined user ID, or
- The user ID is not connected to the group specified in the table

Undefined user IDs for started procedures can be prohibited by coding a generic entry containing a default ID such as */STCDEF/STCGRP and by ensuring that all entries in the table are error-free.

User IDs that are assigned to started procedures should have the PROTECTED attribute. Protected user IDs are user IDs that have both the NOPASSWORD and NOOIDCARD attribute. Protected user IDs cannot be used to logon to the system, and are protected from being revoked through incorrect password attempts.

A Started Procedure can gain access to RACF -Protected Resources in the following ways;

- By the user ID or Group Name assigned, as for any other user of the system.
- By having the Privileged Attribute, which allows the Started Procedure to pass all authorization checking. No installation exits are called, no SMF records are generated, and no statistics are updated. Use this option with extreme caution.

- By having the Trusted attribute, which mean the same as Privileged, except that you can request an audit by using the `SETROPTS LOGOPTIONS` command.

Policy enforcement for all environments can be complemented by monitoring SMF Audit Trails and, if required, by coding a RACINIT exit terminating all requests for establishing a RACF environment for the default user ID.

B.2 Resource protection

The recommended policy requires default protection; that is, the prohibition of access to unprotected (undefined) resources. The techniques used in RACF to implement such policy vary with the type of resource, as described in the following sections.

B.3 Data sets

Default protection for data sets can be activated through `SETROPTS PROTECTALL(FAIL)`. When turned on, unprotected data sets can only be accessed by system-level SPECIAL Users. WARN Mode is available to ease migration.

B.3.1 Transactions and other resources

Default protection over General Resources can be achieved through a variety of controls:

- Program logic in resource managers calling RACF
- Settings in the RACF CDT
- Catch-all profiles with UACC=NONE and restrictive specific access

We recommend catch-all profiles because the logic applied by resource managers may not always be known, and changing CDT entries for existing resource classes may not be desirable.

B.4 Authentication

Policy to establish personal accountability must address User behavior as well as strong technical authentication mechanisms. RACF standard user authentication is based on user-selected passwords; another technique supported is RACF passtickets.

B.4.1 Passwords

Two separate issues must be addressed for RACF passwords, the technique through which passwords are secured when stored in the RACF database and password quality controls.

The recommended standard for password protection is DES encryption. Starting with RACF release 2.1, this is the default. For earlier releases, the RACF exit ICHDEX01 must either be deleted or modified to select DES encryption instead of password hashing.

Password quality controls are `SETROPTS PASSWORD` options, as listed below (together with generally recommended settings):

- rule1(length(6,8) alphanum(1,8) - minimum length 6, alphanumeric with a least one character being numeric
- interval(30) - expiration after 30 days
- history(32) - remember 32 previous passwords
- revoke(3) - revoke ID after 3 invalid password attempts

A related SETROPTS option is:

- inactive(30) - revoke user ID after 30 days of inactivity

B.4.2 Passtickets

RACF offers advanced authentication through Passtickets, which are generated by specific products supporting this form of User authentication.

B.5 Naming conventions

Recommended policy is to establish and enforce adequate naming conventions for all Subjects and Objects. The RACF support of such policy is discussed in the following sections.

B.5.1 Data sets

Native RACF strictly enforces data set high-level qualifier (HLQ) naming conventions; in a PROTECTALL(FAIL) environment, only HLQs that match user IDs or Group Names can be created or accessed. Naming Convention Tables and Exits can be used to transform other naming conventions to the RACF standard.

The enforcement of standards beyond the HLQ is possible but may not always be practical because it limits the use of High-Level Generic Dataset Profiles (such as HLQ.**).

B.5.2 Other resources

The use of catch-all profiles helps enforce naming conventions for general resources; Generic Profiles, if used, must be designed accordingly.

B.5.3 Users and groups

User IDs and Group Names are not controlled by RACF in a way that allows enforcement of local naming standards.

B.6 Ownership

Recommended policy is to assign resource ownership to business managers responsible for an application or business area. RACF practice suggests group ownership of profiles and offers an approximation to policy, provided the group structure reflects applications and business areas adequately and custodians are properly assigned as group administrators.

B.7 Security administration

Recommended policy addresses many aspects of security administration; some can be supported by RACF, as discussed in the following sections.

B.7.1 Structure

Security administration tasks are typically performed within the following structures:

- Central security administration
- Group administration or functional delegation
- Help desk

Mandatory central security administration uses the RACF system-level **SPECIAL** attribute to define or alter all but a few profiles and options in RACF. To set or change some specific audit-related settings requires the system-level **AUDITOR** attribute.

Optional group administration in RACF is based on **Group-SPECIAL**, which provides authority within the scope of a group, or on a privilege called class authorization (CLAUTH), or both. Most policy requirements for group administration can be met by assigning *Group-SPECIAL* and possibly CLAUTH, and by defining the scope of authority (based on Group ownership).

Typical help desk functions such as user ID RESUME and password RESET can be implemented through the RACF FACILITY class, **Group-SPECIAL**, or organizations have chosen other (limited) solutions through special programs that run authorized and use authorization schemes other than **Group-SPECIAL.**

B.7.2 Effectiveness

Recommended policy requires security administration to be effective, i.e., to minimize potential risks through errors and omissions, particularly in the area of temporary access and authorization. Typical precautions are automatic expiration dates on user IDs and permissions. RACF provides the direct ability to expire user IDs automatically through coding **REVOKE(date)** in User definitions; for permissions, expiration dates can be established indirectly through group connections.

B.7.3 Efficiency

Recommended policy also requires security administration to be efficient, to ensure that administration workload problems do not contribute to risks.

Efficient RACF administration uses two main elements: generic profiles, and group authorization on access lists. The use of generic profiles reduces, in comparison with discrete ones, the number of profiles to be defined and maintained. Using groups instead of user IDs on access lists dramatically simplifies the management of a changing user population.

B.8 Audit considerations

Recommended policy requires a reasonably complete audit trail and firm procedures to monitor and review security events and status information.

B.8.1 Logging

RACF provides an audit trail of security-related events through SMF; the nature and amount of information recorded is controlled by RACF options and profile definitions as discussed below:

- `SETROPTS SAUDIT`, `OPERAUDIT CMDVIOL` and `INITSTATS` are the recommended standard settings, which include privileged user activities.
- `AUDIT(SUCCESS(UPDATE) FAILURE(READ))` is the recommended standard profile option, unless specific reasons exist for different settings.
- The RACF global table should not cover any resources for which an audit trail is needed.
- `UAUDIT` should be used rather carefully because, if used generously, it may create a significant amount of noise records.

B.8.2 Event monitoring

Recommended policy requires regular event monitoring. We recommend putting as much emphasis on success as on detected violations. RACF provides four reporting options:

- Data Security Monitor (DSMON) provides “canned” RACF database and z/OS auditing reports.
- The RACF report writer allows for ad hoc violation reporting.
- The RACF database unload utility and SMF unload feature allows you to unload the RACF database and violation records from SMF into flat files.
- The RACFICE reporting tool includes over 30 sample reports, and uses the DF/SORT ICETOOL report generator.

B.8.3 Status review

Recommended policy requires periodic security status monitoring and full security audits. The RACF DSMON utility provides basic event monitoring capabilities. The RACF database unload utility converts SMF records into a format that can be easily processed by a relational database or other tools. For detailed information on RACF reporting tools, see `https://www.ibm.com/products/resource-access-control-facility`.

B.9 Resource utilization

Recommended policy and common sense require that the security monitor’s performance impact be minimal.

B.9.1 Performance options

RACF offers key performance options that should be used in order to comply with policy:

- Resident blocks in the RACF data set name table - recommended value 255
- Global table entries for trivial access in class DATASET - recommended entry &RACUID/ALTER

B.9.2 Potential performance impact

Performance impacts may be caused by the following RACF practices:

- Extensive use of discrete profiles in class DATASET
- Poor use of generic profiles, such as a huge number of profiles under one HLQ
- No global table in large TSO environments

C

Frequently asked questions

Q. When protecting an HLQ for a production application (when there is no user with a corresponding user ID), when should I use a group name for the HLQ and when should I simply create an artificial user ID? Why?

A. Defining a group is the normal approach and this is a normal use for group definitions. We recommend using user IDs only for real users. (Some exceptions exist; artificial user IDs might be used for Started Task Control, for example.) There is no strong technical reason for this recommendation; it is simply that using group IDs provides a more orderly way to manage access to application data sets.

Q. Can I prevent users from permitting access to files they own? How?

A. Yes. The most global way to do this is to remove access to the `PERMIT` command. However, we recommend that you do not do this unless there is a particular, pressing need. Experience has shown little need to hide the `PERMIT` command.

Q. How can I control the number of PERMITs created by a user? Should I worry about this?

A. Again, experience has shown that this is not normally a problem to worry about.

Q. Do I need to reorganize the RACF database? Also the backup database? How often?

A. The IRRUT400 utility can be used to reorganize the RACF database.

Experience has shown that this does not need to be done frequently. Some installations never reorganize their database. Others do it every month or so. Reorganizing every six months seems to be a medial position. The backup database is subject to the same reorganization process.

Q. Can I make simple backups of the RACF database? (Without the complication of using IDCAMS?)

A. IDCAMS is never needed with RACF. You can use the IRRUT200 utility provided with RACF. You could use something as simple as IEBGENER, although IEBGENER (or other similar utilities) will not interlock with RACF to provide a self-consistent copy. IRRUT200 provides the proper interlocks (without effectively stopping RACF) so that partly updated Profiles will not be copied.

Q. Can I administer RACF from CICS?

A. This ability is not part of the basic RACF product. There are third-party tools that provide this ability. Some installations have written their own tools, often based on submitting jobs from CICS (via an internal reader) that executes the appropriate RACF commands. We do not recommend this approach unless you have the skills to assure the security of design. Note that APPC interfaces can also be used to schedule RACF administrative commands.

Q. What authority does a help desk need?

A. A help desk, especially one that is related to a specific set of Departments, is often given access via the RACF facility class parameter or GROUP SPECIAL authority for those departments. This permits the help desk personnel to make almost any RACF adjustments to users who are members of the groups associated with these departments.

There is considerable debate over what authority is appropriate for help desk operations. The trend is to give them less absolute authority, and more tools to perform specific functions. This debate is more related to appropriate security policy than to specific RACF functions.

Q. How do I add a segment to an existing user ID? For example, add CICS to a TSO user?

A. The `ALTUSER` command provides this function.

Q. What do I need to do to share my RACF database between multiple z/OS systems?

A. Nothing; this function is automatic. You need the appropriate shared-DASD hardware, of course. If sysplex functions are available, a higher-performance mode of sharing can be used.

A major difference between Sysplex and a conventional large computer systems is the improved growth potential and level of availability in a Sysplex. The coupling facility allows z/OS and other software to share data concurrently among multiple systems in the Sysplex, with the goal of maintaining a single system image.

Q. Someone gave me some interesting programs that use the RACF `ICHEINTY` set of macros. Should I consider using these?

A. The `ICHEINTY` macro is the low-level interface to the RACF database. At this level, RACF does not check updates for consistency. A poorly designed program issuing these macros could destroy your database, or, worse, introduce subtle errors that grow over time. We recommend not using this level of interface unless you really trust the design of the program issuing the commands, or have a very unusual requirement. There are helpful and trustworthy programs that use `ICHEINTY`, but there is no easy way to determine if your programs are in this trustworthy and useful group.

Q. I want to see my RACF database contents. The TSO commands and ISPF panels only deal with a small number of elements at one time, and I cannot get an overall picture of what is in the database. How can I do this?

A. You can use the RACF database unload utility. With it, you can see every profile in the database, in a printable format. For anything larger than a trivial database, this may not be useful for direct human viewing. It can be used as input to other (locally written) programs, or be used to load Db2 or something similar. The RACF `SEARCH` command can be used to find and display Profiles. The RACFICE reporting tool is available, which includes over 30 sample reports, and uses the DF/SORT ICETOOL Report Generator.

Q. Do I need to train all my users for RACF?

A. Probably not, especially if you have a well-designed group structure and well-designed generic profiles. A relatively short note might be used to inform users about any changes in logon processing.

Your help desk staff and your group Administrators may require more education.

Q. Can I list the passwords of my users? I have SPECIAL authority.

A. RACF can store passwords in two forms: encrypted and hashed. The encrypted form is the default. The hashed form can be recovered; IBM does not provide details about how to do this, but there are many informal programs that do it. We strongly recommend using the encrypted form. There is no way to list the original passwords, once they have been encrypted.

Q. After I install RACF, can I run my z/OS system without it? What if I make a change that locks out users?

A. Once installed, you can run without RACF. This is a very special mode, awkward to use, and suitable for only a single user on the system. In effect, z/OS issues a console message for every data set allocation, and the z/OS operator must reply to each message in order for the user to log on and repair the problem. In addition, the user ID used in this situation must be defined in SYS1.UADS. This is so rarely used that many installations and systems programmers have never experienced the situation.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

Other publications

These publications are also relevant as further information sources:

- *z/OS Security Server RACF System Programmer's Guide,* SA23-2287-30
- *z/OS Security Server RACF Security Administrator's Guide,* SA23-2289-30
- *z/OS Security Server RACF Security Auditor's Guide,* SA23-2290-30
- *z/OS Security Server RACF Command Language Reference,* SA23-2292-30

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

- **ibm.com**/services

Abbreviations and acronyms

ACB	Access Control Block
ACEE	ACessor Environment Element
ACID	ACcessor IDentifier
APPC	Advanced Program-to-Program Communications
API	Application Programming Interface
CBIPO	Custom-Built Installation Process Offering
CDSA	Common Data Security Architecture
CDT	Class Descriptor Table
CICS	Customer Information Control System
CLAUTH	CLass AUTHorization
CLISTS	Command Lists
CMDF	Commercial Data Masking Facility
CPU	Central Processing Unit
DASD	Data Access Storage Device
Db2	Database/2
DCE	Distributed Computing Environment ,component of SecureWay Security Server for z/OS
DDN	Data Definition Name
DES	Data Encryption Standard
DFDSS	Data Facility/Data Storage System
DFP	Data Facility Product
DFSMS	Data Facility/System-Managed Storagey
DLF	Data Lookaside Facility
DNS	Domain Name Services
DSMON	Data Security Monitor
DSN	Dataset Name
EOS	Erase On Scratch
FTP	File Transfer Protocol
GAC	Global Access Checking
GID	UNIX Group IDentifier
GRS	General Resources
HFS	Hierarchical File System
HLQ	High Level Qualifier
ICB	Inventory Control Block
IBM	International Business Machines Corporation
IMS	Information Management System
IPL	Initial Program Load
IPSec	Information Protocol Security
ISPF/PDF	Interactive System Productivity Facility/Program Development Facilityi
ISV	Independent Software Vendor
ITSO	International Technical Support Organization
JCL	Job Control Language
JES	Job Entry Subsystem
LDAP	Lightweight Directory Access Protocol, component of SecureWay Security Server for z/OS
LPA	Link Pack Area
MVS	Multiple Virtual Storage
NAT	Network Address Translation
NDS	Novell Directory Services
NJE	Network Job Entry
OCEP	Open Cryptographic Enhanced Plug-ins, component of SecureWay Security Server for z/OS
OMVS	Open Edition for MVS
OVM	Open Edition for VM
PADS	Program Access to Data Sets
PCICC	PCI Cryptographic Coprocessor
PGM	Program
PKI	Public Key Infrastructure
PL/I	Programming Language/1
RACF	Resource Access Control Facility, component of SecureWay Security Server for z/OS
RJE	Remote Job Entry

RJP	Remote Job Process
RRSF	RACF Remote Sharing Facility
SA	Security Association
SAF	System Authorization Facility
SDSF	System Data Spool Facility
SMF	System Management Facilities
SMPO	Software Migration Project Office
SMS	Storage Management Subsystem
SNA	Systems Network Architecture
SPT	Started Procedures Table
STC	Started Task Control
SYSRES	System-resident pack
TME	Tivoli Management Environment
TMP	Terminal Monitor Program
TSO	Time Sharing Option
UACC	Universal ACCess authority
UADS	User Attribute Data Set
UID	User IDentifier
USS	UNIX System Services
VM	Virtual Machinge
VOL	Volume
VPN	Virtual Private Network
VSAM	Virtual System Access Method
VTAM	Virtual Telecommunications Access Method

To determine the spine width of a book, you divide the paper PPI into the number of pages in the book. An example is a 250 page book using Plainfield opaque 50# smooth which has a PPI of 526. Divided 250 by 526 which equals a spine width of .4752". In this case, you would use the .5” spine. Now select the Spine width for the book and hide the others: Special>Conditional Text>Show/Hide>SpineSize(-->Hide:)>Set

IBM Redbooks

CA TopSecret to
z/OS Security Server Migration
Guide

(1.5” spine)
1.5”<-> 1.998”
789 <->1051 pages

IBM Redbooks

CA TopSecret to
z/OS Security Server Migration Guide

(1.0” spine)
0.875”<->1.498”
460 <-> 788 pages

IBM Redbooks

CA TopSecret to z/OS Security Server Migration Guide

(0.5” spine)
0.475”<->0.873”
250 <-> 459 pages

IBM Redbooks

CA TopSecret to z/OS Security Server Migration Guide

(0.2”spine)
0.17”<->0.473”
90<->249 pages

(0.1”spine)
0.1”<->0.169”
53<->89 pages

To determine the spine width of a book, you divide the paper PPI into the number of pages in the book. An example is a 250 page book using Plainfield opaque 50# smooth which has a PPI of 526. Divided 250 by 526 which equals a spine width of .4752". In this case, you would use the .5” spine. Now select the Spine width for the book and hide the others: Special>Conditional Text>Show/Hide>SpineSize(-->Hide:)>Set

CA TopSecret to z/OS Security Server Migration Guide

(2.5” spine)
2.5”<->nnn.n”
1315<-> nnnn pages

CA TopSecret to z/OS Security Server Migration Guide

(2.0” spine)
2.0” <-> 2.498”
1052 <-> 1314 pages

Broadcom Top Secret and z/OS Security Server

Broadcom Top Secret and the IBM® z/OS® Security Server (RACF®) are both Mainframe Security products. In some areas their designs are similar, and in other areas the designs are very different. Planning a migration from Broadcom Top Secret to z/OS Security Server RACF, without unduly disrupting an z/OS production environment, requires considerable planning and understanding. With proper planning, and perhaps with specially skilled people to assist in certain areas, the migration can usually be accomplished in an orderly way.

This IBM Redbooks® publication will assist in understanding the higher-level issues and differences between the two products as an important starting point.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-5677-01 ISBN DocISBN