z/VM
7.3

Secure Configuration Guide

IBM

SC24-6323-05

Note:

Before you use this information and the product it supports, read the information in “Notices” on page 67.

This edition applies to version 7, release 3 of IBM® z/VM® (product number 5741-A09) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2024-03-08

© Copyright International Business Machines Corporation 2005, 2024.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures....................... vii

Tables....................... ix

About This Document....................... xi
  Who Should Read This Book....................... xi
  Accessing the Certified OSPP Version of this Document....................... xi
  Where to Find More Information....................... xi
    Link to the Certified Product Guidance....................... xi
    Links to Other Documents and Websites....................... xi

How to provide feedback to IBM....................... xiii

Summary of Changes for z/VM: Secure Configuration Guide....................... xv
  SC24-6323-05, z/VM 7.3 (March 2024)....................... xv
  SC24-6323-04, z/VM 7.3 (December 2023)....................... xv
  SC24-6323-04, z/VM 7.3 (September 2022)....................... xv
  SC24-6323-03, z/VM 7.2 (May 2022)....................... xv
  z/VM 7.2 Common Criteria Certification....................... xv
  SC24-6323-01, z/VM 7.2 (September 2020)....................... xv

Chapter 1. Introduction....................... 1
  Introduction to Security Models and Compliance....................... 2
    Securing Virtualization Technology....................... 3
    Labeled Security....................... 3
  Subjects....................... 4
  Objects....................... 5
    Named Objects....................... 5
    Storage Objects....................... 6
    Public Objects....................... 6
  The Systems of Privilege....................... 7
    z/VM Privilege....................... 7
    RACF Privilege....................... 8
    Privilege Interaction....................... 9
  Labeled Security Mode (LSM)....................... 9
    What is a Security Label?....................... 9
    Security Zones....................... 11
    Security Labels and Mandatory Access Control (MAC)....................... 11
    The Rules of MAC....................... 11
    Reserved Security Labels....................... 12
    MAC Using SECLABELs: A Demonstration....................... 12

Chapter 2. Requirements for Installing and Customizing z/VM and RACF....................... 15
  Required Software Levels....................... 15
  Secure System Initialization....................... 15
  Installing and Customizing z/VM....................... 16
    Specify Password Suppression....................... 16
    Prevent Users of T-disks and Minidisks from Seeing Residual Data....................... 16
  Installing and Customizing TCP/IP....................... 17

Required VMSSL Command Operands.......... 17
Required DTCPARMS Operands.......... 17
Required INTERNALCLIENTPARMS Statement Operands.......... 18
Installing and Customizing RACF.......... 18
RACF Installation Steps.......... 18
RACF Customization Steps.......... 20

Chapter 3. Administrative Requirements for z/VM and RACF.......... 27

General Administrative Requirements for z/VM.......... 27
Avoid Modifications to the Configuration.......... 27
CP System Directory Restrictions.......... 27
TCP/IP Restrictions.......... 27
Control z/VM Management Network.......... 28
Restrict Access to the System Console.......... 28
LINK and MDISK Requests Are Subject to DAC.......... 28
Security-Relevant Events Can Produce Unique Audit Records.......... 29
Requirements on Handling Certain Objects.......... 29
Privileged Users Must Be Trustworthy.......... 30
Global Access Checking Bypasses MAC and DAC.......... 30
MDISK Requests Are Subject to MAC.......... 30
The SECLABEL of the Creator of a Logical Device Must Equal That of Any of Its Users or be SYSNONE.......... 31
All Saved Segments and IMG Files Must Be Redefined.......... 31
Considerations for NSSs Defined with the VMGROUP Option.......... 31
Objects Created by z/VM Receive a SYSHIGH SECLABEL.......... 31
Store the Human-Readable Label Table.......... 31
Applying SECLABELs to Every Imported Object.......... 31
Verify SECLABELs Accompanying Data Exported from Your System.......... 32
Unlabeled Spool Files Are Not Accessible in an OSPP-Compliant System.......... 32
TLS Connections Produce Unique Audit Records.......... 32
Handling of Random Number Generation and Validation of Entropy.......... 32
Transferring Spool Files Produce Unique Audit Records.......... 33
Do Not Include Any Sensitive or Classified Data in Broadcast Messages.......... 34
TAG Commands Are Subject to MAC.......... 34
Control of Secondary Users and Observers with MAC.......... 34
Administrative Requirements for RACF.......... 34
Use of Multiple RACF Service Machines.......... 34
Objects in GAC Table and Global Minidisk Table Bypass DAC.......... 35
Performance Considerations.......... 35
Maintain UACC(NONE) in RACF Profiles.......... 35
Audit the Use of RACF Privilege.......... 36
The RACF SETRACF Command Is Always Audited.......... 36
Generating Audit Reports.......... 36
Use of Read-Only Audit.......... 36
Transfer of Audit Records.......... 36
RACF Considerations in an SSI Environment.......... 37

Chapter 4. Additional Topics for LSM.......... 39

CP Printer Support.......... 39
Human Intervention Needed to Meet Common Criteria.......... 39
MAC Protection of CP Printers.......... 39
Human-Readable Labels.......... 40
Map Security Label Character Strings to Human-Readable Labels.......... 41
Random Security Numbers for Print Jobs.......... 43
The RACSEC Program (Querying a User's Current SECLABEL).......... 43
The LOGON Command.......... 44
The CP QUERY READER/PRINTER/PUNCH Command.......... 44

The CP CHANGE Command.......45
DIAGNOSE Code X'BC'.......45
DIAGNOSE Code X'D4'.......46
The CMS RDRLIST Command.......46

Appendix A. Security-Relevant Commands, DIAGNOSE Codes, and System Functions.......49
Security-Relevant CP Commands.......49
DIAGNOSE Codes.......51
System Functions.......52

Appendix B. Security Objectives for the IT Environment.......55

Appendix C. Requirements for the General User.......57
General User — Common Criteria.......57
  Never Leave Your Console Terminal Unattended.......57
  Do Not Add Programs to the System.......57
  Carefully Protect Removable Objects.......57
  Periodically Change Your LOGON Password and Other Credentials.......57
  Protect Your Credentials.......57
  Your Work May Be Audited.......57
  Temporary Disks that You Receive Are Always Cleared.......58
  DIAL, UNDIAL and Pre-LOGON MESSAGE Command Are Not Available.......58
  Directory Changes Must be Synchronized in an SSI Cluster.......58
General User — CC-Secure with LSM.......58
  RACF Controls Access to Minidisks.......59
  MAC Affects the Way You Manage Your Minidisks and Files.......59
  MAC Affects the Way You Send and Receive Data.......59
  Privilege Class G Users Can Purge Any of Their Own Spool Files.......59
  MAC May Cause Some Application Programs to Fail.......59
  Additional Enhancements and Changes.......60

Appendix D. Using HCPRWAC.......61
Add HCPRWAC to the Control Program.......61

Appendix E. Testing the Modified Control Program and Placing it into Production.......63
Testing the Modified Control Program.......63
Placing the New CP into Production.......64

Notices.......67
Programming Interface Information.......68
Trademarks.......68
Terms and Conditions for Product Documentation.......68
IBM Online Privacy Statement.......69

Bibliography.......71
Where to Get z/VM Information.......71
z/VM Base Library.......71
z/VM Facilities and Features.......72
Prerequisite Products.......74
Related Products.......74

Index.......75

Figures

1. A demonstration of MAC using SECLABELs....13

2. An example of a Common Criteria audit record for the TRANSFER command.... 29

3. An example of a Common Criteria audit record for the transfer of a spool file.... 29

4. An example of an OSPP audit record for the TRANSFER command on an LSM system.... 33

5. An example of an OSPP audit record for the transfer of a spool file....33

6. An example of the RDRLIST panel....47

7. An example of the logon prompt.... 58

8. "Update SYSSUF Table Entries" Screen....62

9. Stand Alone Program Loader Screen....64

Tables

1. A hypothetical mapping of SECLABEL character strings to security levels and categories......................11

2. Security Labels for Trusted Servers..23

3. A hypothetical mapping of SECLABEL character strings to security levels, categories, and indentification labels...40

4. Record format for SECTABLE FILE..41

5. Security Relevant CP Commands...49

6. Security Relevant DIAGNOSE Codes.. 51

7. Security Relevant System Functions.. 52

About This Document

This document describes the steps necessary to configure your z/VM installation to conform with the requirements of the Common Criteria.

Who Should Read This Book

This book is designed for administrators responsible for establishing and maintaining security policies on a z/VM system.

Accessing the Certified OSPP Version of this Document

The formally certified OSPP version of this document, SC24-6232-02, can be downloaded from this URL:

https://www.vm.ibm.com/library/720pdfs/72632302.pdf

The site that controls and maintains this document (the "IBM z/VM 7.2 PDF files" web page) uses HTTPS to assure transmission of its contents.

Before downloading the PDF version of this document, please verify the validity of the certificate being used to secure your web connection. The mechanism for validating a certificate will vary depending upon the web browser being used to download the document (for example, by clicking on the padlock icon in Microsoft Internet Explorer, then choosing "More Information" and "Security" to view the contents of the certificate, or by selecting Tools > Page Info > Security > View Certificate in Mozilla Firefox.

The certificate should indicate an Organization of "IBM," with a Common Name (CN) of "*.ibm.com".

If you are unable to locate a certificate, or cannot find a valid or correct certificate, you may not be viewing the appropriate level of guidance. Please refer to on-site help information or contact IBM Support with any comments or questions.

Where to Find More Information

See "Bibliography" on page 71.

Link to the Certified Product Guidance

A .ZIP file containing the PDF format versions of documentation relevant to configuring a z/VM 7.2 system is available on IBM Resource Link at this URL: https://www.vm.ibm.com/library/720pdfs/2020-3q.zip.

Links to Other Documents and Websites

The PDF version of this document contains links to other documents and websites. A link from this document to another document works only when both documents are in the same directory or database, and a link to a website works only if you have access to the Internet. A document link is to a specific edition. If a new edition of a linked document has been published since the publication of this document, the linked document might not be the latest edition.

© Copyright IBM Corp. 2005, 2024

How to provide feedback to IBM

We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information. See How to send feedback to IBM for additional information.

© Copyright IBM Corp. 2005, 2024

Summary of Changes for z/VM: Secure Configuration Guide

This information includes terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations for the current edition are indicated by a vertical line (|) to the left of the change.

SC24-6323-05, z/VM 7.3 (March 2024)

This edition includes changes to support product changes provided or announced after the general availability of z/VM 7.3.

[VM66732] Digital Signature Verification of z/VM Service Packages

With the PTF for APAR VM66732, z/VM 7.3 uses public-key cryptography to verify the authenticity and integrity of signed service packages.

The following topic is updated:

- "Installing and Customizing z/VM" on page 16

SC24-6323-04, z/VM 7.3 (December 2023)

This edition includes terminology, maintenance, and editorial changes.

SC24-6323-04, z/VM 7.3 (September 2022)

This edition supports the general availability of z/VM 7.3.

SC24-6323-03, z/VM 7.2 (May 2022)

This edition adds further clarification for adherence to the NIAP Virtualization Protection Profile (VPP) 1.0, with Server Virtualization Extensions. Because the VPP evaluation represents a superset of functionality when compared to the previous z/VM 7.2 evaluation, most of what appears in SC24-6323-02 (referenced below) pertains to both evaluations. However, additional updates were required to assure strict compliance with this Profile.

z/VM 7.2 Common Criteria Certification

z/VM 7.2 will be certified to conform to the Operating System Protection Profile (OSPP) with Virtualization (-VIRT) and Labeled Security (-LS) extensions of the Common Criteria standard for IT security, ISO/IEC 15408, at Evaluation Assurance Level 4 (EAL4+). Additionally, z/VM 7.2 will be certified to conform to the NIAP Virtualization Protection Profile (VPP) 1.0, with Server Virtualization Extensions.

SC24-6323-02, z/VM 7.2 (February 2021): This guidance has been updated to provide a single common configuration context for all security measures to which z/VM 7.2 might apply.

For more information about this announcement, see IBM z/VM Security and Integrity Resources (https://www.ibm.com/vm/security).

SC24-6323-01, z/VM 7.2 (September 2020)

This edition supports the general availability of z/VM 7.2.

© Copyright IBM Corp. 2005, 2024

Chapter 1. Introduction

Attention:

- Conformance to the requirements of the Common Criteria is determined solely by an independent evaluation and certification by accredited organizations and signatory government agencies.

  The SC24-6232-02 edition of this book has been certified to be compliant with the Common Criteria. That edition can be downloaded from this URL:

  https://www.vm.ibm.com/library/720pdfs/72632302.pdf

  The SC24-6232-03 edition of this book has been certified to be compliant with the NIAP Virtualization Protection Profile (PP_BASE_VIRTUALIZATION_V1.0). That edition can be downloaded from this URL:

  https://www.vm.ibm.com/library/720pdfs/72632303.pdf

  The site that controls and maintains this document, IBM z/VM 7.2 PDF files (https://www.vm.ibm.com/library/720pdfs.html), uses HTTPS to assure transmission of its contents.
- Refer to IBM z/VM Security and Integrity Resources (https://www.ibm.com/vm/security) for a link to current evaluation plans and status.
- z/VM 7.1 is designed to comply with the same Common Criteria requirements as were successfully evaluated for z/VM 6.4.
- z/VM 6.4 was evaluated against the requirements of the Common Criteria Operating System Protection Profile (OSPP), BSI-CC-PP-0067, Version 2.0 (dated 2010-06-10), including the extended packages of OSPP:
  - Virtualization (OSPP-VIRT), Version 2.0
  - Labeled Security (OSPP-LS), Version 2.0

  This protection profile was designed as a replacement for the discontinued Controlled Access Protection Profile (CAPP). It takes into account today's environments, in which networked systems often process specialized tasks, use cryptographic services, and provide distributed security services.
- The z/VM system must be configured in a Single System Image (SSI) configuration, and must have been created using the IBM-provided installation instructions for SSI configurations.

The **Common Criteria** was developed by several national security standards organizations in the United States and other countries, in concert with the International Organization for Standards (ISO). Common Criteria Version 2.1 is now formally recognized as ISO 15408, a world standard for security specifications and evaluations.

For more on Common Criteria, see The Common Criteria Portal (www.commoncriteriaportal.org).

An integral part of the Common Criteria is the **Protection Profile** (PP), an implementation-independent set of security requirements and objectives for a category of products or systems which meet similar needs for IT security.

For more on protection profiles, see National Information Assurance Partnership (NIAP) (www.niap-ccevs.org/).

The **Target of Evaluation (TOE)** is that part of the product or system which is subject to evaluation. The TOE security threats, objectives, requirements, and summary specification of security functions and assurance measures together form the primary inputs to the **Security Target (ST)**, which is used by the evaluators as the basis for evaluation.

The Common Criteria has provided seven predefined assurance packages, on a rising scale of assurance, known as **Evaluation Assurance Levels (EALs)**. These provide balanced groupings of assurance

© Copyright IBM Corp. 2005, 2024

components that are intended to be generally applicable. Not all government schemas issue EALs, and not all Protection Profiles include them.

Note that the evaluated configuration requires that the RACF Security Server feature of z/VM be enabled and used. It also requires that the Single System Image function (previously a feature of z/VM) be used.

Introduction to Security Models and Compliance

General purpose operating systems often operate in environments that provide centralized services which can be used by a large number of systems within an organization. It is expected that a modern general purpose operating system will provide the capability to use centralized services for the implementation of security functionality – for example, authentication servers, directory servers, certification services, or audit log servers. While most modern general purpose operating systems implement functions such as centralized security services, they may also be able to act as the server for those services. Therefore some systems must have the capability to act as a server for a centralized security service. Cooperating with another trusted IT system to provide a security service is not restricted to the use of centralized services, but can also be accomplished in a peer-to-peer relationship. One example is the authentication of a human user that is based on a token that the user needs to present. (This could be a smartcard, for example.) In this scenario, the user authenticates to the smartcard using his or her PIN, and then the smartcard authenticates the user to the operating system by presenting the user's certificate and assuring the operating system that it has the private key associated with the public key in the certificate.

Operating systems conformant to the Common Criteria are assumed to operate in an environment in which the platform on which they execute (hardware, devices and firmware) is protected from physical attacks and manipulation. In addition, it is assumed that all management activities are performed by knowledgeable and trustworthy users. (See Appendix B, “Security Objectives for the IT Environment,” on page 55.)

In z/VM, these security requirements are met through the following specific mechanisms:

- **Discretionary Access Control (DAC)**

  A method of restricting access to data objects based upon the identity of users or groups to which the users belong. DAC protects system objects from unauthorized access by any user. Normally, permission to access an object is granted by the owner of the object; occasionally, it can be granted by someone else, such as a privileged administrator.

- **Auditability of Security-Relevant Events**

  The recording of facts that describe a security-relevant event taking place in a computing system. In general, a security-relevant event is one that occurs in a computing system that, for better or for worse, affects the safety and integrity of the system's processes and data.

  The facts recorded that describe such an event include the time and date of the event, the name of the event, the name of the system objects affected by the event, the name of the user who caused the event to occur, and additional information about the event.

  In general, the security-relevant events in z/VM are:

  - CP commands
  - DIAGNOSE functions
  - Communication among virtual machines.

- **Object Reuse**

  A practice that prevents any newly-assigned storage object from making available to its new owner any data that belonged to its former owner. This includes any encrypted data.

  Object reuse also requires the elimination of any residual user authorization access to a previously existing object. This ensures that if another, new object occurs in the system later under the same name, the subjects having access to the old object will not have access to the new one.

- **Identification and Authentication**

A method of enforcing individual accountability by providing a way to authenticate a user's identity uniquely and unambiguously. Thus, any security-relevant action users might take can be attributed to them.

z/VM 7.2 has added one extended package to its conformance to the VPP base and two extended packages to its conformance to the OSPP base. Virtualization is applicable to both, through the specific mapping is distinct for each package.

Securing Virtualization Technology

A hypervisor, by virtue of its position in the data center, adds requirements that will allow execution of multiple, separated compartments on a single trusted system. Each compartment can behave like a single platform, separated from other compartments. The system enforces this separation and controls communication between compartments, as well as communication with external entities, in accordance with a defined policy. As such, compartments are a different set of active entities, in addition to the subjects defined for operating system security models. The following implementations of virtualization functionality provided with general purpose operating systems are covered:

- **Hardware virtualization**

  Hardware virtualization utilizes the hardware, mainly the processor support of a hypervisor state, in addition to the supervisor and user states. The hypervisor state is provides an isolated operating space for itself and operating spaces for other untrusted entities. These untrusted entities can then use the supervisor and user states of the processor. For this implementation, a compartment is a separated entity capable of executing a standard operating system.

- **Operating system functionality virtualization**

  The operating system compartmentalizes the user space to provide strict isolation of the user space compartments. Within these compartments, processes can communicate as usual. However, processes located in different compartments are not allowed to perform any communication. This implementation defines a compartment as a collection of processes (subjects as defined in the OSPP base) that are isolated from other collections of processes according to the policy defined for the virtualization mechanism.

- **Server virtualization functionality**

  Server Virtualization (as defined by the NIAP SVPP extended package) implements virtualized hardware components on server-class hardware. It creates a virtualized hardware environment for each instance of an operating system (virtual machines or VMs), permitting these environments to execute concurrently while maintaining isolation and the appearance of exclusive control over assigned computing resources. Each VM instance supports applications such as file servers, web servers, and mail servers. Typically, virtualized servers provide services to remote clients and are generally not directly accessible by non-administrative users.

Labeled Security

Note:

The packages used by z/VM 7.2 for evaluation require an additional set of functions that will be defined here collectively as labeled security mode (LSM). The LSM-specific information will be clearly marked with the following tags:

LSM_Begin

LSM_End

If the LSM-specific information is not appropriate to your system, then these sections can be skipped.

LSM_Begin

Labeled security defines protecting information in multilevel environments. Multilevel security is a security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. A multilevel-secure security policy has two primary goals. First, the controls must prevent unauthorized individuals from accessing information at a higher classification than their authorization would allow. Second, the controls must prevent individuals from declassifying information. The security functionality of this package applies to all users and all untrusted subjects, as well as all named objects.

To meet these requirements, the overall functionality is augmented with the following key additions:

- **Security Labeling**

  A system of assigning a label to each subject and object that signifies its confidentiality and its membership in a security category. RACF uses these security labels to decide whether a subject gets access to an object. Most of the security labels are defined by the system administrator; others are assigned default values based on the type of the object. When an object is imported to or exported from the system, the system must unambiguously associate the object with a security label. Further, each printed object must conspicuously display the human-readable label associated with its security label.

- **Mandatory Access Control (MAC)**

  A security policy that governs which subjects can access which objects, and in what way, based upon the relationship between their security labels. MAC restricts a subject's access to an object based upon three things:

  - The security label of the subject
  - The security label of the object
  - The type of access the subject wants.

If the MAC criteria are met, z/VM then performs DAC.

MAC is based on the Bell-LaPadula security model, which consists of the *-property (star property, also known as the confinement property), and the simple security property.

The *-property security model rule allows a subject write access to an object only if the security label of the subject is dominated by the security label of the object.

The simple security property security model rule allows a subject read access to an object only if the security label of the subject dominates the security label of the object.

For more information on how z/VM enforces these principles, see "Labeled Security Mode (LSM)" on page 9.

LSM_End

Subjects

A subject is an active entity in a computing system that either causes information to flow among objects or changes the system's state.

In z/VM, a subject is a virtual machine — one of four types:

- General user
- Privileged user
- Trusted server
- System operator.

Each has approximately the same logical structure.

A general user is defined as a virtual machine which:

- Has *at most* the CP commands available in IBM-defined privilege class G. (It may have fewer.)
- Does *not* have SPECIAL, group-SPECIAL, CLAUTH, group-CLAUTH or OPERATIONS authority to RACF.
- Does *not* have COMSRV, DIAG88, DIAG98, DEVMAINT, MAINTCCW, or SETORIG options in its CP directory entry.
- Does *not* have OBEY authority for VM TCP/IP.
- Does *not* have access to the z/VM directory (source or object forms).

- Does *not* have read-write access to the PARM disk(s), or other system areas of CP-owned volumes.
- Does *not* have read-write access to the source or object code of CP, CMS, RACF, or z/VM TCP/IP.
- Does *not* have read-write access to the RACF database.
- Does *not* have read-write access to the RACF audit trail.
-
- If multi-factor authentication is enabled, does *not* have have password fallback enabled.
- Is *not* the secondary console of any user that does not meet the above requirements.

All other virtual machines are considered to be Administrators.

A privileged user is any user (for example, a system or security administrator) who is allowed to bypass the security policies of z/VM. These include, but are not limited to, users with CP privilege other than class G, and RACF users with the SPECIAL attribute. See "z/VM Privilege" on page 7 for more on privilege classes.

A trusted server or trusted service virtual machine is a machine that runs programs necessary to the system's operation. These programs provide services such as security, networking, and directory management. A trusted server typically runs disconnected.

The system operator or system operator's virtual machine is considered a privileged subject, though not a trusted one. It is allowed certain special privileges, such as sending and receiving messages without a MAC check (see "Security Labels and Mandatory Access Control (MAC)" on page 11). The system operator virtual machine is not considered trusted because it does not run disconnected.

Similarly, a virtual machine set up to run batch jobs is not a trusted server. Although it runs disconnected, it always performs work on the behalf of another user and does not run programs necessary to the system's operation.

Objects

An object is a passive entity in a computing system that contains or receives information. Minidisks, spool files, saved segments, and virtual memory are some examples of objects. Access to an object implies access to the information it contains. In general, to create, delete, access, or move an object is to cause a security-relevant event to occur, which may require auditing and control.

The security criteria for the Common Criteria standards forbid any newly-assigned object from making available to its new owner any data that belonged to its former owner. What's more, these criteria forbid any residual authorization to access objects that no longer exist. For example the system will clear any data from a temporary disk before assigning the disk to the new owner.

z/VM uses several types of objects, as described below.

Named Objects

A named object is an object that can be directly manipulated by z/VM. It can also be manipulated by or for a user who is not the owner of the object. In this case, the user manipulating the named object must be granted the correct access to the object.

The following is a list of named objects:

- Minidisks
- Real Devices
- Guest LANs and Virtual Switches
- Spool files and System Data files
- Discontiguous Saved Segments (DCSS)
- Named Saved Segments (NSS)
- Virtual machine address spaces
- Virtual machine communication facility (VMCF) buffers

- Inter-User Communication Vehicle (IUCV) buffers
- Advanced Program to Program Communication/Virtual Machine (APPC/VM) buffers
- Virtual Channel-to-Channel Adaptor (VCTCA) buffers
- CP MESSAGE command buffers.

Storage Objects

A storage object is an object that supports both READ and WRITE access, though not necessarily for the same user at the same time.

The following is a list of storage objects:

- Minidisks
- Spool files and System Data files
- DCSSs
- NSSs
- Address spaces
- Temporary disks (T-disks)
- Virtual memory
- Guest LANs and Virtual Switches

Note: It is possible for a named object to be a storage object, too. Further, it is possible for a subject to act like an object. For example, if one user sends a message to another user, the user receiving the message is an object.

Public Objects

A public object is an object to which all subjects have READ-ONLY access, but to which only privileged subjects have READ/WRITE access. Since z/VM permits all subjects to have READ/ONLY access, no access control decision is necessary, and the event need not be auditable. All other operations, however, are subject to access control and audit.

To enhance performance, z/VM makes public objects available as READ-ONLY and without audit. The system protects public objects from being created, modified, or deleted, except by users which have been given the “proper” privilege, or access, by the system administrator.

The following is a list of public objects:

- Log messages (LOGMSGs)
- Logon logos
- Objects listed in the RACF global access checking (GAC) table
- Minidisks listed in the RACF global minidisk table.

A saved segment is a group of one or more memory segments that has been previously loaded, saved, and assigned a unique name.

A log message (LOGMSG) is a message from the system administrator, or system operator, that appears on the screen every time a user logs on.

A logon logo is the “hello” screen which begins a terminal session; it contains identification information on the software product. The information on the logo screen can be changed for a particular installation, therefore, the rules on who can create, modify, or delete information apply. Logo information is similar to a log message.

Global access checking (GAC) is the first test performed by RACF to determine whether a subject should have access to an object and, if so, what kind of access. GAC checks a table that lists a group of objects and the kind of access that any subject in the system can gain to it. If the object appears in the GAC table, the subject immediately receives the sort of access listed. For additional information on GAC, see

"Objects in GAC Table and Global Minidisk Table Bypass DAC" on page 35. To define an object to the GAC table, see *z/VM: RACF Security Server Security Administrator's Guide*.

The global minidisk table identifies the minidisks in your installation that can be considered public disks. A public disk is a disk that has the following characteristics:

- Allowed READ access by all users of the system
- Used by the majority of users on the system
- Contains no sensitive data.

Attention: In z/VM, objects in the GAC table and global minidisk table are not subject to DAC or RACF auditing. (Although objects in the GAC table can be audited using the VMXEVENT auditing for the LINK command.)

The Systems of Privilege

In general, privilege is a particular level of authority given to users that allows them to perform certain tasks while preventing them from performing others. Each component of z/VM has its own particular system of privilege, and each system of privilege has its own particular security implications. In some cases, these individual systems of privilege interact with each other.

z/VM Privilege

In the z/VM system of privilege, a user can have no privileges, or be assigned to one or more privilege classes. Each privilege class represents a subset of CP commands that the system permits the user to enter.

Each privilege class, sometimes called CP privilege class, is defined around a particular job or set of tasks, thereby creating an area outside of which the user may not go. Of course, it is commonplace for a user to be assigned to more than one CP privilege class. Users are unable to enter commands in privilege classes to which they are not assigned.

Note: Any user, except those with either NO PRIVILEGE or CP privilege class G, is considered part of the configuration, but is not necessarily considered trusted.

A summary of CP privilege classes, their associated users, tasks, and security implications follows:

Privilege class A – The primary system operator

The system operator is among the most powerful and privileged of all z/VM users. The system operator is responsible for the system's availability and its resources. The system operator also controls accounting, broadcasts messages, and sets performance parameters.

Privilege class B – The system resource operator

The system resource operator controls the allocation and de-allocation of real resources, such as memory, printers, and DASD. Note that the system resource operator does not control any resource already controlled by the system operator or the spooling operator.

Privilege class C – System programmer

A system programmer updates the functions of the z/VM system and can change real memory in the partition.

Privilege class D – Spooling operator

The spooling operator controls spool files and real unit record devices, such as punches, readers, and printers.

Privilege class E – System analyst

The system analyst has access to real memory and examines dumps to make sure that the system is performing as efficiently and correctly as possible.

Privilege class F – IBM service representative

A representative of IBM who diagnoses and solves problems by examining and accessing real input and output devices and the data they handle.

Privilege class G – General user

This is the most prevalent and innocuous of the CP privilege classes. The commands that privilege class G users can enter effect only their own virtual machines.

Privilege class ANY

The commands in this privilege class are available to any user.

It should be obvious from the discussion above that privilege classes A, B, C, D, E, and F, require individuals worthy of very significant trust and whose activities require careful auditing.

For example, users with privilege class B or C can modify an installation's system of CP privilege. Or as another example, privilege class C users can enter the CP STORE HOST command, allowing them to alter real memory. Because in both cases the Common Criteria security policy claims would be violated (regardless of Protection Profile in use), system programmers and similarly privileged users must be "trusted" to not tamper (and auditing must confirm this) with the system of CP privilege.

Privilege class G users have no influence outside their own virtual machines. So, with the exception of access to storage objects, they have very little security relevance.

The ANY privilege class commands cannot violate the security policies of the system. This is because all commands in the ANY privilege class are auditable and subject to either discretionary or mandatory access control, DAC or MAC. (See "Security Labels and Mandatory Access Control (MAC)" on page 11.) Therefore, class ANY users, together with class G users, cannot violate the security policy.

In CP, each level of privilege is discrete and not predicated on others. Furthermore, each privilege class (a subset of commands) is related to one or more function types (subsets of users). To learn more about privilege classes and function types, see *z/VM: CP Commands and Utilities Reference*. To learn about CP command and DIAGNOSE protection through RACF, see *z/VM: RACF Security Server Security Administrator's Guide*.

Privilege Class Modification

The privilege classes assigned to CP commands and DIAGNOSE codes may be changed by an installation provided no additions are made to the set of commands and DIAGNOSE codes included in class G as defined and shipped by IBM. Commands and DIAGNOSE codes may be removed from class G as desired.

RACF Privilege

As in CP, each level of RACF privilege is discrete and not predicated on others. A summary of RACF privilege classes follows:

SPECIAL

Gives the user full control over all profiles in the RACF database. If the SPECIAL attribute is assigned at the group level, the group-SPECIAL user has full control over all RACF profiles within the scope of the group.

Users with the SPECIAL attribute are allowed to log on while the system is in a tranquil state. This is necessary to perform administrative tasks such as changing security labels.

OPERATIONS

Gives the user full authorization to RACF-protected resources that do not specifically exclude users with the OPERATIONS attribute. If the OPERATIONS attribute is assigned at the group level, then the group-OPERATIONS user has full control over all RACF-protected resources within the scope of the group.

AUDITOR

Gives the user authorization to specify auditing and logging options within RACF profiles. If the AUDITOR attribute is assigned at the group level, then the group-AUDITOR user's authority is limited to his or her own group.

ROAUDIT (Read-Only Auditor)

Gives the user authorization to view, but not to modify, audit log content and audit seeings. If the ROAUDIT attribute is assigned at the group level, then the group-ROAUDIT user's authority is limited to his or her own group.

CLAUTH
Allows the user to define profiles in RACF for classes of previously defined or installation-defined resources.

Note: The books in the RACF library refer to these privilege classes as user attributes. The term privilege class is used in the book you are reading now for consistency across all of the products. To learn more about RACF user attributes, see *z/VM: RACF Security Server Security Administrator's Guide*.

Privilege Interaction

It is important to recognize that trusted servers often give their administrators more privilege than the administrator has on his or her own. For example, the NETSTAT CP command, available to users in the TCP/IP "obey" list, allows the TCP/IP administrator to issue an arbitrary CP command within the TCPIP virtual machine. The TCPIP virtual machine has, by default, privilege class B. Ensure that a user is not inadvertently given more privilege than he or she needs. In the TCP/IP example, giving a user OBEY authority so that the user could issue the TRACERTE command would implicitly give that user class B capabilities. (It is for this reason that the TCP/IP server audits all uses of NETSTAT CP.)

Note:

The rest of this chapter is devoted to LSM-specific information. If this is not appropriate to your system, please go directly to Chapter 2, “Requirements for Installing and Customizing z/VM and RACF,” on page 15.

Labeled Security Mode (LSM)

LSM_Begin

Central to z/VM is its system of security labeling.

Each object in an LSM-compliant z/VM system has a security label, or “SECLABEL,” that designates its relative confidentiality and its membership in a security category. An object's security label defines what sort of data it can contain and, by implication, what sort of data it cannot contain. Note that an object can have one and only one security label at any given time.

Similarly, each user (subject) in the system has at least one security label that designates relative power and privilege over objects. That is, a subject's security label specifies whether it can access a given object and, if so, what actions, if any, it can perform upon that object. Some subjects perform a wide variety of tasks and fulfill many different roles, each with its own security implications; so it is only natural that some subjects be able to perform work under more than one security label each. Note, however, that only one security label can be in effect at any given time, and it governs all of the subject's activity until it is changed.

A security relationship, then, always exists between the SECLABEL of any given subject and the SECLABEL of any given object. Within this relationship, the security relationship between subject and object itself is implied. A question to consider is, “Is this relationship conducive to the security of the organization?” The answer to that question is provided by mandatory access control, which is discussed in “Security Labels and Mandatory Access Control (MAC)” on page 11. But first, more about SECLABELs.

What is a Security Label?

A security label is a simple, one- to eight-byte, installation-defined character string. This character string represents the union of a security level with zero or more security categories. A maximum of 254 security levels and 32,767 security categories can be defined on your system, or 8,323,768 SECLABELs!

A security level specifies into which general order of sensitivity and confidentiality a subject, or object, falls. These levels exist in a hierarchy defined by your installation.

The following sections illustrate the general concept of SECLABELs, using the U. S. Department of Defense hierarchy of security levels. In descending order of sensitivity, these security levels are:

1. TOP SECRET (TOPSEC)

2. SECRET (SECRET)
3. CONFIDENTIAL (CONF)
4. UNCLASSIFIED (UNCL)

A security category specifies which area of information a subject is permitted to access or an object is permitted to contain. Again, security categories are defined by the individual installation; unlike security levels, however, no hierarchy is implied among security categories. They are nothing more than areas of knowledge.

Your installation designs its system of SECLABELs after a careful analysis of its processes, personnel, and data. Then, at installation time, the system administrator defines a mapping from SECLABEL character strings to the security levels and categories for which each character string stands. Study the following hypothetical mapping:

Table 1. A hypothetical mapping of SECLABEL character strings to security levels and categories.

SECLABEL Character String	The Security Level	The Security Categories
SECL1	TOPSEC	PROJA PROJB PROJC
SECL2	SECRET	PROJC PROJD PROJE
SECL3	CONF	PROJB
SECL4	CONF	PROJD PROJE
SECL5	CONF	PROJE

For example,and object protected by SECL1 contains information protected at the TOP SECRET level, and pertains only to PROJECTS A, B, and C. Nothing more! And, a subject governed by SECL1 is, similarly, limited in its activities by mandatory access control, which will be discussed next.

Note: It is possible to have different security labels defined with identical security levels and categories. The MAC policy, covered in detail in the following sections, discusses security label comparisons. It is important to note that these comparisons are based on the complete composition of the security label (more specifically, the security level and security category), and are not just a comparison of the 8-character security label character strings.

Security Zones

Security labels can be used to implement "security zones," in which a z/VM user ID can access only the resources defined as belonging to the same zone. This includes minidisks, virtual channel-to-channel adapters, spool files, guest LANs, and virtual switches (and, hence, OSAs). When virtual machines are in different zones, no inter-virtual machine communication is permitted, whether through shared memory, CP system services, or CP commands.

Security Labels and Mandatory Access Control (MAC)

Mandatory Access Control (MAC) is a security policy that governs which subjects can access which objects, and in what way, based upon certain rules. These rules are the “*-property” and the “simple security property.”

RACF commands are used to manage MAC for CP commands, DIAGNOSE codes, and system functions. MAC restricts a subject's access to an object based upon three things:

- The security label of the subject
- The security label of the object
- The type of access the subject requires for the task being performed.

If MAC criteria are met, z/VM then performs discretionary access control (DAC), where appropriate.

The Rules of MAC

In z/VM, all MAC decisions are made by RACF, and are subject to the following rules.

The Domination Rule

The SECLABEL of a subject dominates that of an object if two conditions prevail: (This is also an example of the “*-property.”)

- The subject's security level is greater than (that is, more sensitive), or equal to, that of the object
- All the security categories of the object are found among those of the subject.

Likewise, the SECLABEL of an object dominates that of a subject if two conditions prevail:

- The object's security level is greater than, or equal to, that of the subject

- All the security categories of the subject are found among those of the object.

The READ-ONLY Rule

If a subject wants READ-ONLY access to an object, such as a LINK to a disk in RR mode, the SECLABEL of the subject must dominate that of the object. This prevents a subject from “reading up,” which means to read data from an object that has a more sensitive SECLABEL — a violation of the security policy. (This is also an example of the “simple security property.”)

The WRITE-ONLY Rule

If a subject wants WRITE-ONLY access to an object, the SECLABEL of the object must dominate that of the subject. This prevents a subject from “writing down,” which means to write data in an object that has a less sensitive SECLABEL — also a violation of the security policy.

The READ/WRITE Rule

If a subject wants READ/WRITE access to an object, two conditions must prevail:

- The subject's security level must exactly equal the security level of the object
- The security categories of the subject must be precisely the same as those of the object.

Reserved Security Labels

Following is a list of security labels that are reserved for use by the system. These security labels have specific implications in the enforcement of MAC.

SYSHIGH
The security label consisting of the highest security level and all of the security categories.

SYSLOW
The security label consisting of the lowest security level and none of the security categories.

SYSNONE
This security label is used to bypass label checking for the subject or object. It should be assigned only to trusted users who provide system-wide services. For example, TCPIP must be assigned SYSNONE to allow users with different security labels to access the system using the same telnet server.

NONE
The character string NONE must *not* be used as a security label because:

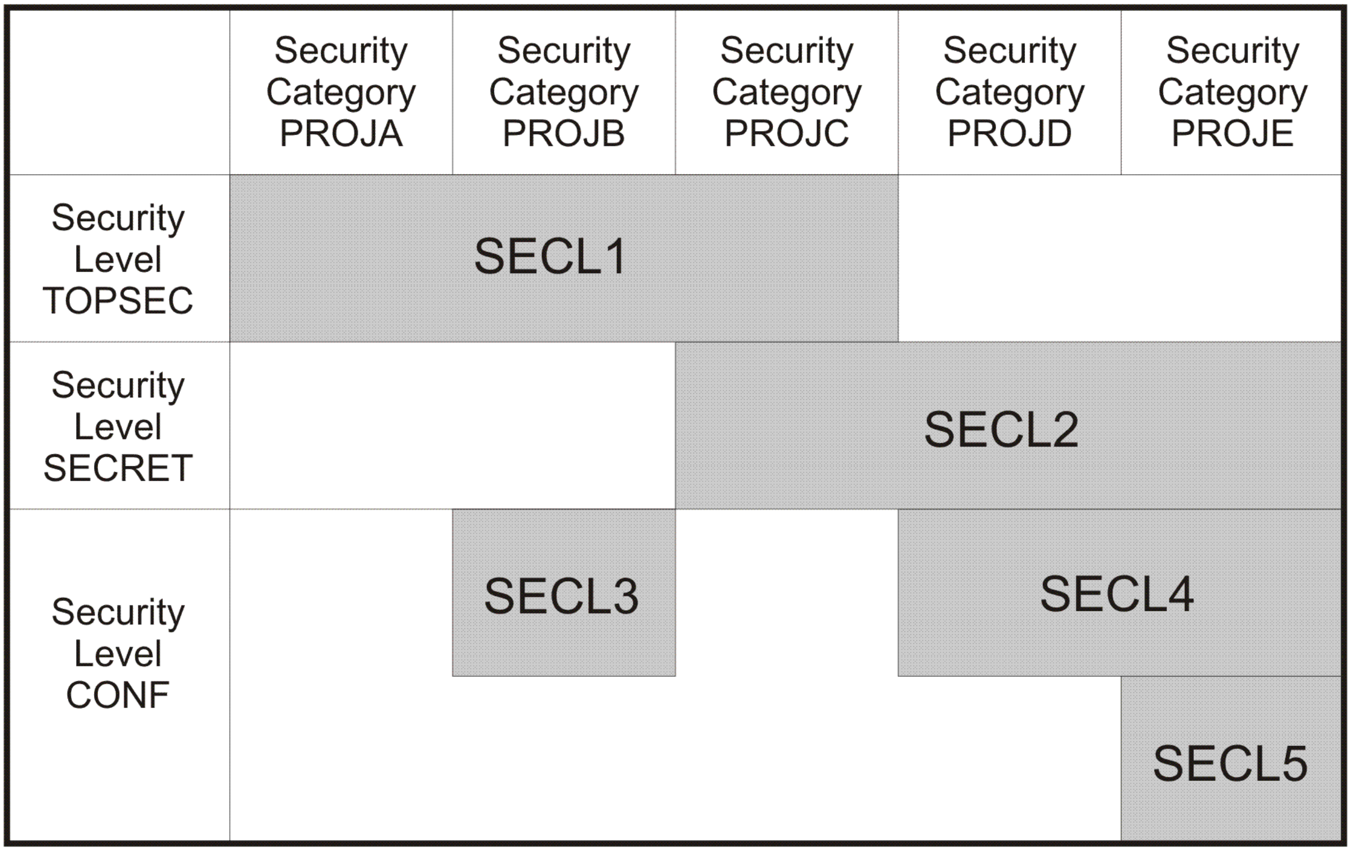
- This is the default security label for VM system printers. CP prevents jobs from printing on a printer with a security label of NONE.
- If an object has no security label, the word NONE appears in the SECLABEL field of the response to the QUERY READER/PRINTER/PUNCH and QUERY TRFILES commands.

MAC Using SECLABELs: A Demonstration

To understand the relationship between the rules of MAC and SECLABELs, let's consider a concrete example. Figure 1 on page 13 illustrates two things:

- The relationship between the security level and security category within each of several SECLABELs
- The relationship among the SECLABELs.

Note the SECLABELs represented by the shaded areas, each bearing its identifying character string.



<table>
<tr><th></th><th>Security Category PROJA</th><th>Security Category PROJB</th><th>Security Category PROJC</th><th>Security Category PROJD</th><th>Security Category PROJE</th></tr>
<tr><td>Security Level TOPSEC</td><td colspan="3">SECL1</td><td></td><td></td></tr>
<tr><td>Security Level SECRET</td><td></td><td></td><td colspan="3">SECL2</td></tr>
<tr><td rowspan="2">Security Level CONF</td><td></td><td>SECL3</td><td></td><td colspan="2">SECL4</td></tr>
<tr><td></td><td></td><td></td><td></td><td>SECL5</td></tr>
</table>

Figure 1. A demonstration of MAC using SECLABELs

Consider “The Rules of MAC” on page 11 and Figure 1 on page 13 as you review the following questions:

Q: Can a subject governed by SECL1 perform a READ-ONLY operation on an object protected by SECL2?

A: No. Although the security level of the subject is greater (more sensitive) than that of the object, all the categories of the object are not among those of the subject.

Q: Can a subject governed by SECL1 perform a READ-ONLY operation on an object protected by SECL3?

A: Yes. The security level of the subject dominates that of the object, and all the categories of the object are found among those of the subject.

Q: Can a subject governed by SECL1 perform a READ/WRITE operation on an object protected by SECL1?

A: Yes. The subject's security level is exactly equal to that of the object, and the security categories of the subject are exactly the same as those of the object.

Q: Can a subject governed by SECL2 perform a READ/WRITE operation on an object protected by SECL1?

A: No. First, the security level of the subject does not exactly equal the security level of the object. Second, although the subject and object do have one security category in common, the others are not precisely the same.

LSM_End

Chapter 2. Requirements for Installing and Customizing z/VM and RACF

This chapter describes the security requirements to keep in mind while installing or customizing z/VM and RACF. Use the options and restrictions described in this chapter to configure z/VM and RACF to be compliant with the requirements of the Common Criteria protection profiles under use. If you want to operate your system in labeled security mode (LSM), additional information is provided. Note that the LSM specific information in this chapter is clearly marked. If this is not appropriate for your system, you may skip these items

Required Software Levels

z/VM has been evaluated only with the RACF® Secure Server and Single System Image features enabled.

RACF is necessary because it provides all of the authentication, authorization, and audit functions required by modern enterprise security. Security servers other than RACF do not provide the functionality used by LSM and have not been evaluated for their compliance. While z/VM can be operated with an external security manager of any sort, such a configuration does *not* meet the requirements specified by the Common Criteria packages under use.

The RACF Security Server feature is pre-installed on z/VM, but not enabled. Consult the z/VM RACF Program Directory for information on enabling RACF.

Additionally, another server must be added in support of multi-factor authentication. RACF/VM supports use of IBM Z® Multi-factor Authentication 2.1, running in a Linux® on IBM Z guest. Consult documentation for that product in order to install and configure MFA.

Similarly, the Single System Image feature is also pre-installed on z/VM, but not enabled. Consult the z/VM Program Directory for information on enabling the Single System Image feature.

For OSPP compliance: In order to make sure you have the correct version of z/VM 7.2, make sure you have applied service level 7201RSU and the PTF for APAR PH24751 (for FIPS 140-2 compliance).

For VPP compliance: In order to make sure you have the correct version of z/VM 7.2, ensure that you have applied service level 7201RSU, the PTF for APAR PH24751 (for FIPS 140-2 compliance), the PTF for APAR PH28216 (for OCSP support), and the PTF for APAR VM66540 (for direct-to-host download support).

To ensure that your system contains only genuine IBM software:

- Install z/VM only from physical media provided by IBM (DVD) or from electronic media obtained from IBM Shopz.
- Install any needed service only from physical media provided by the IBM Support Center or from electronic media obtained from official IBM online support portals.

Secure System Initialization

Between the time you initialize z/VM and the time you initialize RACF, the virtual machines that are autologged during z/VM initialization run without the auditing and control of RACF.

By default, these virtual machines include:

AUTOLOG1
DISKACNT
OPERATOR
EREP
OPERSYMP

© Copyright IBM Corp. 2005, 2024

To prevent anyone from taking advantage of this interval, take the following precautions:

- Specify the DRAIN and DISABLE options when CP asks you for the type of start you want to perform. (For additional information, see “Bringing Up the System” in *z/VM: System Operation*.)
- Be certain that the AUTOLOG1 virtual machine enables only the RACF service virtual machines and no others. AUTOLOG2 will be started by RACF after it has completed its initialization. Everything you would normally place in AUTOLOG1 should be placed in AUTOLOG2 instead.
- Do not enable your general-use console terminals (with CP ENABLE) or the TCP/IP stack and its associated services until after you initialize RACF. Until then, enable only the system console and keep it under strict physical security.

Installing and Customizing z/VM

Before proceeding, make sure z/VM is at the software level described in “Required Software Levels” on page 15. Individual z/VM PTFs must be applied according to the instructions in "Chapter 3. Installing preventive or corrective service" in the *z/VM: Service Guide*.

An administrator can download service directly from IBM ShopZ. The GETSHOPZ utility handles certificate verification when connecting to IBM Shopz to download service, and it validates digital signatures to ensure the authenticity and integrity of downloaded service. (The hash calculation for ordered service is also sent to the associated account for additional corroboration.) GETSHOPZ can also be used to validate digital signatures when uploading from a workstation or if the service was transferred in another manner. For more information about the GETSHOPZ utility, see the *z/VM: Service Guide* and the GETSHOPZ information on the IBM z/VM Service web page (https://www.vm.ibm.com/service/getshopz.html).

With the PTF for APAR VM66732 applied, the following security-related requirements are addressed:

- Common Criteria Virtualization Protection Profile v1.1+, requirement for Trusted Update (FPT_TUD_EXT.1). The update to z/VM requires a digital signature within certain cryptographic specifications, which must be validated before new code is installed.

  Administrators and system programmers can be assured that the service they receive from IBM was not tampered with in transit. This function uses the certificate to validate the signature.
- Trusted service and hashing requirements for the IBM Z family of servers.

GETSHOPZ programmatically validates the authenticity and data integrity of the package that is downloaded from ShopZ. It is highly recommended that the ordering system programmer also verify the data to correlate that package with the hash value received in the ordering email. This is to ensure that the package has not been modified in transit or after arriving on the z/VM system. The system programmer must not install IBM packages that come from a source other than IBM. It is additionally recommended that the system programmer install no packages that arrive without a hash value or that cannot be verified independently by a human user of the system.

For more information about the following initialization requirements, see *z/VM: CP Planning and Administration*.

Specify Password Suppression

Password suppression prevents any password from being visible on the terminal screen. To enable password suppression, place the following statement in the SYSTEM CONFIG file (this statement is the default):

```
FEATURES PASSWORDS_ON_CMDS AUTOLOG NO LINK NO LOGON NO
```

Prevent Users of T-disks and Minidisks from Seeing Residual Data

You must ensure that each time the system assigns T-disk space, it clears the space of all residual data. To ensure this, place the following statement in the SYSTEM CONFIG file:

```
FEATURES ENABLE CLEAR_TDISK
```

Note: CLEAR_TDISK is enabled by default in z/VM 7.2, if not specified. However, anyone updating their z/VM SYSTEM CONFIG file should validate that the CLEAR_TDISK feature is enabled (and not disabled).

Further, before a minidisk is assigned to a user, the minidisk must be formatted to clear it of any residual data. CMS FORMAT, ICKDSF, or any other low-level formatting program that erases all of the data on the minidisk may be used.

Installing and Customizing TCP/IP

Required VMSSL Command Operands

The Transport Layer Security (TLS) server allows secure communication between two TCP/IP connection participants. If your system is using TLS or Secure Socket Layer (SSL), you must ensure that the appropriate VMSSL command operands are specified, as only certain cipher suites are appropriate in a Common Criteria compliant system:

```
PROTOCOL TLSV1_2
PROTOCOL +TLSV1_1
PROTOCOL -TLSV1_0
PROTOCOL -SSLV3
EXEMPT DES_56_SHA
EXEMPT DHE_RSA_DES
EXEMPT DHE_DSS_DES
```

Alternately, if strict adherence to FIPS 140-2 evaluation levels are required inside your installation, use the following VMSSL command operands instead:

```
MODE FIPS-140-2
PROTOCOL TLSV1_2
PROTOCOL -TLSV1_1
PROTOCOL -TLSV1_0
PROTOCOL -SSLV3
EXEMPT DES_56_SHA
EXEMPT DHE_RSA_DES
EXEMPT DHE_DSS_DES
EXEMPT ECDH_ECDSA_NULL_SHA
EXEMPT ECDH_ECDSA_RC4_128_SHA
EXEMPT ECDH_ECDSA_3DES_EDE_SHA
EXEMPT ECDH_ECDSA_AES_128_SHA
EXEMPT ECDH_ECDSA_AES_256_SHA
EXEMPT ECDHE_ECDSA_RC4_128_SHA
EXEMPT ECDH_RSA_NULL_SHA
EXEMPT ECDH_RSA_RC4_128_SHA
EXEMPT ECDH_RSA_3DES_EDE_SHA
EXEMPT ECDH_RSA_AES_128_SHA
EXEMPT ECDH_RSA_AES_256_SHA
EXEMPT ECDHE_RSA_RC4_128_SHA
EXEMPT ECDH_ECDSA_AES_128_SHA256
EXEMPT ECDH_ECDSA_AES_256_SHA384
EXEMPT ECDH_RSA_AES_128_SHA256
EXEMPT ECDH_RSA_AES_256_SHA384
EXEMPT ECDH_ECDSA_AES_128_GCM_SHA256
EXEMPT ECDH_ECDSA_AES_256_GCM_SHA384
EXEMPT ECDH_RSA_AES_128_GCM_SHA256
EXEMPT ECDH_RSA_AES_256_GCM_SHA3
EXEMPT RSA_AES_128_GCM_SHA256
EXEMPT RSA_AES_256_GCM_SHA384
EXEMPT DHE_RSA_AES_128_GCM_SHA256
EXEMPT DHE_RSA_AES_256_GCM_SHA384
EXEMPT DHE_DSS_AES_128_GCM_SHA256
EXEMPT DHE_DSS_AES_256_GCM_SHA384
TRACE CONNECTIONS NODATA
```

See *z/VM: TCP/IP Planning and Customization* for more information on the VMSSL command.

Required DTCPARMS Operands

The TLS server is programmatically defined in the DTCPARMS file. If your local security policy or Common Criteria compliance requires the Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) definitions, add the :OCSP_Parms. tag to your TLS server definition.

For more information about OCSPENABLE and CDPENABLE, refer to *z/VM: TCP/IP Planning and Customization*.

Required INTERNALCLIENTPARMS Statement Operands

If your system is using SSL and you wish to configure the Telnet server to provide secure connectivity to z/VM, you must ensure that the appropriate INTERNALCLIENTPARMS operands are enabled:

SECURECONNECTION
determines if validation of a server's certificate has been performed. Set this operand to `REQUIRED` to mandate secured Telnet traffic only.

CLIENTCERTCHECK
determines if validation of a client's certificate has been performed by the z/VM SSL Server. Set this operand to `REQUIRED` to validate every client's certificate.

TLSLABEL
specifies the certificate label required for the server certificate.

See *z/VM: TCP/IP Planning and Customization* for more information on the INTERNALCLIENTPARMS statement.

Installing and Customizing RACF

Using the z/VM RACF Program Directory as a reference, use this section to install and initialize RACF.

Before proceeding, ensure RACF is at the software level described in "Required Software Levels" on page 15. If applicable, individual RACF PTFs must be applied according to the instructions in Chapter 7 of the z/VM RACF Program Directory.

For z/VM Single System Image (SSI) installation, you must manually define the primary and backup RACF databases as two 3390 full-pack minidisks. It is required that the RACF database be shared between the members of an SSI cluster. See the "Sharing RACF Databases in a z/VM Single System Image Cluster" section of the *z/VM: RACF Security Server System Programmer's Guide*. See also *z/VM: CP Planning and Administration* for more information on DASD sharing.

Note that in the z/VM RACF Program Directory, some LINK commands issued prior to the use of RACF require a password immediately following the LINK mode (such as MR or RR). For new installations, the default RR minidisk password is *read* and the MR minidisk password is *multiple*.

Use the instructions in Step 1 of "Chapter 14. Install Preventive (RSU) or Corrective (COR) Service and Place the Service into Production" in the *z/VM: Installation Guide*. Do not place RACF into production yet as additional modifications to RACF are required.

To ensure that the system is not accessed from remote locations before all needed configuration has been completed, temporarily modify AUTOLOG2's PROFILE EXEC so that TCPIP is not started. Access via directly attached terminals can be prevented by issuing CP DISABLE ALL. This will be undone in step "12" on page 25.

RACF Installation Steps

Note:

When RACF is installed in an SSI cluster, you need to perform steps **6.5.1**, "Deleting the ICHRCX02 Exit," **6.8**, **6.10**, **6.11.1**, **6.12**, **6.13**, and "Testing the Modified Control Program" on page 63 from only one member of that cluster if ICHRCX02 has been installed. ICHRCX02 is not enabled by default in z/VM 6.4 and subsequent releases.

For step **6.6** and "Placing the New CP into Production" on page 64, you must perform these steps on every member of the SSI where this new release of CP and RACF are to be copied into production.

Perform the steps found in Chapter 6 of the z/VM RACF Program Directory, up until **6.5.1**. At that point, proceed using the following modifications and additions:

- **6.5.1**: After running RPIDIRCT, modify the resulting RPIDIRCT SYSUT1 file in the following ways:
  - Alter the VMRDR profile for MAINT720 to specify UACC(UPDATE)
  - Add any additional PERMITs required.
- **6.6**: Set the SMF record (audit trail) archiving policy. To force an archive whenever the primary or secondary SMF disk fills, alter RACFSMF's PROFILE EXEC to specify SMFFREQ = "AUTO" and SMFSWTCH = "NO".

  If an audited security-relevant event occurs, RACF creates an audit record describing the event. This audit record contains such information as the name of the event, who started it, upon what object, when it happened, and so forth. RACF immediately records the audit record in the SMF DATA files. The RACFSMF user ID and the SMFPROF EXEC are provided with RACF to archive SMF data.

  If both the primary and secondary SMF minidisks unexpectedly become full, then no more audit records can be recorded, even though security-relevant events can continue to occur. Naturally, any such loss of audit records is unacceptable in a secure system. The RACF SEVER option can prevent any loss of audit data under these circumstances. SEVER orders the connection between CP and RACF be cut whenever the SMF DATA files become full. To specify this option, modify the one and only record in the SMF CONTROL file to read like this:

  ```
  CURRENT 301 K PRIMARY 301 K SECONDARY 302 K 4096 VMSP CLOSE 001 SEVER YES 0 RACFSMF
  ```

- If ICHRCX02 is enabled on your system (note that ICHRCX02 is not enabled by default in z/VM 6.4 and subsequent releases), follow the instructions in the "Deleting the ICHRCX02 Exit" section of Chapter 6. RACF Installation Exits in *z/VM: RACF Security Server System Programmer's Guide*. Here you are disabling batch-mode surrogate users by deleting ICHRCX02 from RACFLPA LOADLIB.
- **6.7**: Skip this step.
- **6.8**: Enable RACF and place the RACF-enabled CP kernel on MAINT720 CF2.
- **6.9**: Skip this step.
- **6.10**: IPL the RACF-enabled CP kernel from MAINT720 CF2.
- **6.11.1**: Initialize the RACF database.

  Optionally, define a new security administrator user ID and revoke access to IBMUSER.

  Note: When RACF is installed in a single-member or multiple-member z/VM SSI environment, it is mandatory that the RACF database be configured as shared.
- Prepare to use the Common Criteria validated version of CP that is included with z/VM by following the instructions in Appendix D, “Using HCPRWAC,” on page 61. This version of CP contains an IBM-built version of HCPRWA (HCPRWAC). Note that when HCPRWAC is used:
  - RACF will not participate in z/VM POSIX UID and GID management. All requests for POSIX UID and GID information will be obtained from the CP directory.
  - All minidisks will be subject to RACF access control and auditing.
  - The VMMDISK, VMRDR, VMLAN, and VMCMD classes must be active and all resources used within those classes must be defined to RACF. The resource must be defined using a discrete or generic profile (if available), or by placing an entry in the RACF global access table.
  - Passwords for RACF command sessions are not required.
  - The designated RACF services machines are RACFVM and RACMAINT.
- **6.12**: Skip this step. You can update the RACF global access table at any time.
- **6.13**: Activate the resource classes used by RACF service procedures. Log on to the RACF server administrator userid and use the RAC SETROPTS command to enable controls for minidisks, spool files, shared segments, and the use of DIAGNOSE X'D4':

  ```
  rac setropts classact(vmmdisk vmrdr vmbatch vmsegmt)
  ```

- **6.14 and 6.15**: Skip these steps.
- **Test and Place into Production.** Test the Common Criteria enabled version of CP and, if satisfied, place into production. Follow the instructions in Appendix E, “Testing the Modified Control Program and Placing it into Production,” on page 63.

  At this point, all CP changes have been made. No more IPLs are needed.

RACF Customization Steps

Note:

When customizing the RACF security server for z/VM in an SSI cluster, you need to perform these steps from only one member of that cluster.

1. **CP DIAL and MSG**

   Prevent the CP DIAL and MESSAGE (MSG) commands from being used prior to LOGON:

   ```
   RAC  SETEVENT  NODIAL  NOPRELOGMSG
   ```

2. **Define Password Encryption Policy**

   Passwords on z/VM systems are encrypted by RACF for z/VM in order to protect authentication credentials from offline attacks against the security policy stored in the database. RACF for z/VM 6.4 provides two password encryption algorithms: a LEGACY mode and a new KDFAES mode. Note the following:

   - KDFAES requires the enablement of CPACF (hardware feature 3863) for every member of the Single System Image cluster. KDFAES cannot be used if that feature is not enabled.
   - Password encryption strength is set for all z/VM systems sharing the RACF database. For the z/VM Target of Evaluation, this is every member of the Single System Image cluster.

   Select the password encryption setting which best applies to your security policy. If you choose to enable KDFAES, issue the following command:

   ```
   SETROPTS PASSWORD(ALGORITHM(KDFAES))
   ```

   Otherwise, do not change this setting.

3. **Define Password Policy**

   To meet OSPP-enabled version of CP requirements, all passwords must be at least seven characters in length and contain at least one numeric character, not in the first or last position. Further, the user's access to the system must be revoked if five incorrect passwords are entered in a row. The following PASSWORD settings implement this policy:

   ```
   SETROPTS PASSWORD(REVOKE(5)
          RULE1(LENGTH(7:8) ALPHA(1,7) ALPHANUM(2:6))
          RULE2(LENGTH(8) ALPHA(1,8) ALPHANUM(2:7)))
   ```

   To meet VPP conformance claims, use password phrases instead of passwords. A minimum password phrase length of 15 characters shall be supported, and shall allow for any combination of upper and lower case characters, digits, and the special characters "!, @, #, $, %, ^, &, *, (, or)".

   Note: Password phrases may be used in addition to (or instead of) passwords, if desired. Because password phrases are 14 to 100 characters in length, are mixed case, and may contain characters not allowed in a standard password (including blanks), the rules required for passwords do not apply to password phrases. Because the hash symbol # has special operational meaning to the z/VM Control program, exercise extreme caution if attempting to use this symbol as part of a password phrase.

4. **Establish Auditing and Logging Options**

   There are many ways to establish your logging and audit options. You can specify auditing for:

   - Particular resources

- Particular RACF resource classes
- Particular CP commands, DIAGNOSE codes, or system functions
- Particular user or users
- Modifications to RACF profiles.

LSM_Begin

You may also specify auditing for a particular SECLABEL.

LSM_End

For details, see *z/VM: RACF Security Server Auditor's Guide*.

5. **Create RACF Resource Profiles**

   For each of the classes to be activated from the list in the next step, create RACF resource profiles to protect the objects in your system. For information on creating profiles in the other resource classes, see *z/VM: RACF Security Server Security Administrator's Guide*.

6. **Activate Resource Classes**

   The SETROPTS CLASSACT option specifies those resource classes for which RACF protection is activated (see "5" on page 21). In z/VM, the following classes must be activated (some of these classes were activated during RACF installation – activate the rest of them now):

   FACILITY
   Allows a virtual machine to use the RACROUTE interface.

   VMXEVENT
   Permits auditing and protection of CP commands, DIAGNOSE codes, and virtual machine communication. Auditing is permitted for all of these items while protection is permitted for only a subset of these items. For information on which items must be protected in z/VM, see Appendix A, "Security-Relevant Commands, DIAGNOSE Codes, and System Functions," on page 49.

   VMCMD
   Activates the protection of a subset of CP commands.

   VMSEGMT
   Activates protection of DCSSs and NSSs.

   VMRDR
   Activates protection of all unit record devices.

   VMBATCH
   Activates protection of alternate user IDs.

   VMLAN
   Activates protection of guest LANs and virtual switches, including IEEE VLAN identifiers.

   VMMDISK
   Activates protection of minidisks.

   VMDEV
   Activates protection of real devices.

   Note:

   Steps 6-10 apply to systems using LSM. If this is not appropriate to your system, please go directly to step "12" on page 25.

7. LSM_Begin **Define Your Installation's SECLABELs**

   To define your installation's SECLABELs, use the following commands. Note that these are examples only, and are consistent with Figure 1 on page 13.

   First, define your security levels and security categories:

```
RAC RDEF SECDATA SECLEVEL ADDMEM(TOPSEC/200 SECRET/100 CONF/10)
RAC RDEF SECDATA CATEGORY ADDMEM(PROJA PROJB PROJC PROJD PROJE)
```

Next, define the relationships between those security levels and security categories. That is, define your installation's SECLABELs:

```
RAC RDEF SECLABEL SECL1 SECLEVEL(TOPSEC) ADDCATEGORY(PROJA PROJB PROJC)
RAC RDEF SECLABEL SECL2 SECLEVEL(SECRET) ADDCATEGORY(PROJC PROJD PROJE)
RAC RDEF SECLABEL SECL3 SECLEVEL(CONF) ADDCATEGORY(PROJB)
RAC RDEF SECLABEL SECL4 SECLEVEL(CONF) ADDCATEGORY(PROJD PROJE)
RAC RDEF SECLABEL SECL5 SECLEVEL(CONF) ADDCATEGORY(PROJE)
```

For additional information, see *z/VM: RACF Security Server Security Administrator's Guide*.

⚠ **Attention:** Be certain that you define your system's SECLABELs and assign them to users and resources before you activate the RAC SETROPTS MLACTIVE(FAILURES) option. To recover from such a situation, log on as a user with the RACF system-SPECIAL attribute, specifying SYSHIGH as the current security label. Then either assign security labels, or enter SETROPTS NOMLACTIVE.

8. **Assign Users and Trusted Servers Their SECLABELs**

   To authorize a user to perform work under a given SECLABEL, enter the following command:

   ```
   RAC PERMIT seclabel CLASS(SECLABEL) ID(user) ACCESS(READ)
   ```

   Assign a default SECLABEL to each RACF user profile to allow the user to log on without specifying a SECLABEL. Use the following command:

   ```
   RAC ALTUSER userid SECLABEL(seclabel)
   ```

   For example, to authorize user LAURIE to use security label SECL1 and to make SECL1 the default, use these commands:

   ```
   RAC PERMIT SECL1 CLASS(SECLABEL) ID(LAURIE) ACCESS(READ)
   RAC ALTUSER LAURIE SECLABEL(SECL1)
   ```

   For trusted servers, if you adhere to the following procedure, the z/VM RACF administrator sets the security labels for the following virtual machines as follows:

Table 2. Security Labels for Trusted Servers

Virtual Machine	**Security Label**
OPERATOR	SYSHIGH
AUTOLOG1	SYSHIGH
AUTOLOG2	SYSHIGH
Any RACF service machine	SYSHIGH
RACFSMF	SYSHIGH
TCPIP	SYSNONE
Any SFS server machine	SYSNONE

Note: Any user that is autologged by RACF is granted the privilege (by default) to autolog other users without a MAC check.

To bring this about, perform the following procedure, using the *z/VM: RACF Security Server Security Administrator's Guide* as a reference:

a. Establish a USER profile for each of the virtual machines listed above
b. Declare the default SECLABEL of each to be SYSHIGH or SYSNONE, as appropriate
c. Enter the PERMIT command for each of these virtual machines, allowing each to perform work under the SYSHIGH or SYSNONE SECLABEL. For example:

```
PERMIT SYSNONE CL(SECLABEL) ID(TCPIP) ACCESS(READ)
ALTUSER TCPIP SECLABEL(SYSNONE)
```

9. **Assign a Security Label to Each Object**

All objects, including spool files, must have valid security labels. To assign a SECLABEL to a spool file, use the CHANGE command. See "The CP CHANGE Command" on page 45.

Note: Spool files created while running in an OSPP-compliant system automatically acquire the security label of their creator. Security labels must be manually set for pre-existing and imported spool files.

If you do not assign a SECLABEL to a spool file, it can be purged, but it cannot be read or printed.

Resources in the following RACF classes are required to have security labels assigned:

- VMDEV
- VMLAN
- VMMDISK
- VMSEGMT
- WRITER

To assign a security label to a profile which protects a resource, use the following command:

```
RAC RALTER class-name profile-name SECLABEL(security-label)
```

For example, to assign a security label of SECL1 to the 191 minidisk belonging to user ID, LAURIE, you would use this command:

```
RAC RALTER VMMDISK LAURIE.191 SECLABEL(SECL1)
```

The security administrator can assign security labels to resources before the SECLABEL class is activated. The security labels will not be used for authorization checking until the SECLABEL class is activated.

For additional information on assigning security labels, see *z/VM: RACF Security Server Security Administrator's Guide*.

10. **Map Each Security Label to a Human-Readable Label**

    Each SECLABEL declared in RACF must be recorded in the SECTABLE FILE. This file maps each SECLABEL to a human-readable label. OSPP security criteria require that the appropriate human-readable label appear conspicuously on every document printed under a SECLABEL.

    The OSPP security policy requires that the SECLABELs declared in RACF be kept synchronized with those mapped to human-readable labels in the SECTABLE FILE. No security label should appear in the SECTABLE FILE unless it also appears in the RACF database. For additional information on the SECTABLE FILE, see "Map Security Label Character Strings to Human-Readable Labels" on page 41.

11. **Activate SECLABEL Controls**

    The following resource classes must be activated:

    SECLABEL
    Activates security label checking

    VMMAC
    Activates protection of MAC-only z/VM events. No profiles are required in this class.

    WRITER
    Activates protection of printers.

    To activate the SECLABEL resource class and cache the definitions in memory, enter the following RACF commands:

```
RAC SETROPTS CLASSACT(SECLABEL)
RAC SETROPTS RACLIST(SECLABEL)
```

    Note: After you have entered the RACLIST command against the SECLABEL class, any profile therein that is changed is not updated until you enter the following command:

```
RAC SETROPTS RACLIST(SECLABEL) REFRESH
```

    You must also activate the following RACF SETROPTS options. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

    SECLABELCONTROL
    This option prevents users who do not have the SPECIAL privilege from doing either of the following:

    - Specifying or changing a SECLABEL in a resource profile
    - Changing the profiles named SECLEVEL or CATEGORY, or changing any profile in the SECLABEL class such that the definition of a SECLABEL changes.

    Note: Of course, every user can change their own SECLABEL whenever they want, but they must:

    - Stay within the range of SECLABELs set for them by the system administrator
    - Log off and then log on again under the new SECLABEL.

    MLACTIVE(FAILURES)
    This option directs RACF to require a SECLABEL on all subjects and RACF-protected objects in your system. FAILURES specifies that RACF is to reject any request to access an object that does not have a SECLABEL. For details, see *z/VM: RACF Security Server Security Administrator's Guide*.

    ⚠ **Attention:** Be certain that you define your system's SECLABELs and assign users to them before you activate this option. To recover from such a situation, log on as a user with the RACF system-SPECIAL attribute, specifying SYSHIGH as the current security label. Then either assign security labels, or enter SETROPTS NOMLACTIVE, or access SECLABEL-protected resources.

MLS(FAILURES)

This option prevents users from copying data from one subject to another subject with a less sensitive security label. FAILURES specifies that RACF is to reject any request to declassify data in this way.

MLSTABLE

This option prevents any user from changing a SECLABEL definition, or the SECLABEL of an object, unless the system is in a tranquil state.

- All users of the SECLABEL have logged off
- You have entered the RAC SETROPTS MLQUIET command.

LSM_End

12. **Enable Remote and Local System Access**

    Issue these commands on every member of the SSI:

    ```
    CP XAUTOLOG TCPIP
    CP ENABLE ALL
    ```

Chapter 3. Administrative Requirements for z/VM and RACF

This chapter describes the requirements for the administrator of a Common Criteria-compliant z/VM system. Note that the LSM-specific information in this chapter will be clearly marked. If this is not appropriate to your system, you can skip these items.

General Administrative Requirements for z/VM

Avoid Modifications to the Configuration

Your organization may wish to modify the evaluated configuration to meet local needs; however, any modification to the explicitly listed CP and RACF configuration invalidates the certification of the system.

RSUs or PTFs identified by IBM as having been evaluated may be applied in their entirety.

CP System Directory Restrictions

Apply the following restrictions to the CP system directory:

- Do not use the DEDICATE statement in the system directory to dedicate console terminals unless they are under the strictest physical supervision.
- CP commands issued using the COMMAND directory statement run with full system privileges, just as though the command was issued by the system administrator. Use of the COMMAND statement is audited under the control of the DIRECTRY_CMD system event.
- Do not allow any of the following directory control statements (or operands or options on the directory control statements) to appear in the CP system directory entry of any non-trusted virtual machine in the system:
  - CONSOLE with the userid operand
  - IUCV with the ANY or *IDENT RESANY operand
  - OPTION with any of the following operands:
    - COMSRV
    - DEVMaint
    - DIAG88
    - DIAG98
    - D84NOPAS
    - MAINTCCW

  Note: These options are allowed (and some may even be required) for trusted virtual machines in z/VM, but must be removed from all non-trusted virtual machines.
- Do not define a user with a password of NOPASS.
- Do not allow minidisk extents to overlap, except when used for system backup purposes, as this may expose users to data that they are not authorized to see.
- Network services *must not* allow anonymous access to the system or its resources. For example, the TCP/IP DTCPARMS configuration files MUST NOT contain any occurrences of `:Anonymous.YES.`

TCP/IP Restrictions

Apply the following restriction to TCP/IP:

© Copyright IBM Corp. 2005, 2024

- Network services *must not* allow anonymous access to the system or its resources. For example, the TCP/IP DTCPARMS configuration files MUST NOT contain any occurrences of `:Anonymous.YES`.

Control z/VM Management Network

You must maintain logical security controls and network definitions to separate z/VM administrator access to the z/VM system from data networks used by guest workloads. Guests will often use a z/VM Virtual Switch to configure subnets of traffic and communicate via Layer 2 to IBM Z or IBM LinuxONE networking hardware.

It is recommended that traffic to the z/VM system be defined on a separate VLAN from guest traffic. It is encouraged (but not required) that the z/VM TCP/IP stack be configured to use a distinct OSA port from guest network traffic associated with a Guest LAN or a z/VM Virtual Switch; alternately, a z/VM Virtual Switch in VEPA mode will physically separate traffic out through a physical switch somewhere outside IBM Z hardware. (Such a switch would have a firewall configured, and would thus enforce security boundaries for the enterprise based upon larger TOE Environment requirements.)

Additionally, a distinct network of channel-to-channel (CTC) adapters in an ISFC collection serves to connect member nodes of a z/VM single system image cluster. Access to operations around CTC management must be constrained to authorized human users and associated userids; and z/VM Control Program commands associated with single system image maintenance may be audited if required by local security policy.

Restrict Access to the System Console

You MUST maintain physical and logical security controls to protect the Hardware Management Console. If remote operations are permitted, then proper network protections (such as firewalls) SHOULD be implemented. If `SYSTEM_USERIDS OPERATOR` *`operator`* `DISCONNECT` is not specified in SYSTEM CONFIG, then the operator consoles defined in the OPERATOR_CONSOLES statement in SYSTEM CONFIG MUST be protected by physical and logical security controls.

There are certain restrictions that you must place on your system operator:

- You must ensure a high level of physical security over the system console for the processor. This is where the system operators do most of their work.
- The system administrator must observe the rules governing the clearing of objects before they are assigned to new owners. Common Criteria conformance requires that before any object is given to a new owner, it must be cleared of any data belonging to the former owner.

  Note: The system operator can be audited; the system operator does not have to be audited. (See *z/VM: RACF Security Server Security Administrator's Guide* for information on setting up individual z/VM event profiles.)

LINK and MDISK Requests Are Subject to DAC

Any attempt by any virtual machine to link to a minidisk is subject to DAC by RACF. This is true for all LINK and MDISK requests (assuming you have not altered the default VMXEVENT profile). Note that in MDISK requests, users are making link requests to minidisks they already own (i.e. are already in their directory).

If access to a minidisk is requested, and if RACF denies the request, then the link request fails.

Note: In the case of MDISK and LINK requests: If RACF authorizes MR or WR access, CP downgrades the request if another user already has the disk in write mode. The machine receives read-only access to the minidisk, but only if so authorized.

When downgrading occurs, an additional audit record is generated. An access mode of RR indicates that read-only access was granted. XX indicates that the link failed.

For additional information on the LINK command, see *z/VM: CP Commands and Utilities Reference*. For additional information on the MDISK directory statement, see *z/VM: CP Planning and Administration*.

Security-Relevant Events Can Produce Unique Audit Records

The security administrator can select which security-relevant events are to be audited. This section looks only at one event — the transfer of a spool file. For additional information on auditing, see the *z/VM: RACF Security Server Auditor's Guide*. For a list of security-relevant events, see Appendix A, “Security-Relevant Commands, DIAGNOSE Codes, and System Functions,” on page 49.

If auditing is enabled for the TRANSFER command, the event is audited when a user enters the TRANSFER command, and again when the spool file is actually transferred from one unit record device to another. See Figure 2 on page 29 and Figure 3 on page 29 for examples of the format of each of these audit records.

```
                                                        E
                                                        V  Q
                                                        E  U
                     *JOB/USER  *STEP/    --TERMINAL--  N  A
 DATE    TIME   SYSID   NAME     GROUP       ID    LVL  T  L
90.274 22:30:22 VMSP   USERG                         0  2  0

JOBID=(USERG 00.000 00:00:00),USERDATA=(USERG),OWNER=
AUTH=(NONE),REASON=(VMAUDIT)
VMXEVENT=TRANSFER SFCM    0395 TO JSMITH   -,LEVEL=00
```

Figure 2. An example of a Common Criteria audit record for the TRANSFER command.

```
                                                        E
                                                        V  Q
                                                        E  U
                     *JOB/USER  *STEP/    --TERMINAL--  N  A
 DATE    TIME   SYSID   NAME     GROUP       ID    LVL  T  L
90.274 22:30:22 VMSP   USERG                         0  2  0

JOBID=(USERG 00.000 00:00:00),USERDATA=(USERG),OWNER=
AUTH=(NONE),REASON=(VMAUDIT)
VMXEVENT=TRANSFER SFBSTART = 01BA1500,LEVEL=00
```

Figure 3. An example of a Common Criteria audit record for the transfer of a spool file

Note: On system using LSM, the format of these audit records will be significantly different. See “Transferring Spool Files Produce Unique Audit Records” on page 33.

Requirements on Handling Certain Objects

The following facts and requirements apply to certain objects in your system:

Format New Minidisk Space

If your organization decides to convert DASD space (such as spool space, T-disk space, or page space) to permanent minidisk space, then it is the responsibility of the system administrator to clear the entire space of all data. This prevents a new owner of the space from seeing any residual data left by the former owner.

Protect All Dumps from Unauthorized Disclosure

A system dump is a “snapshot,” taken at a particular moment, of the contents of the memory being used by CP for itself and for virtual machines. System dumps may be created by highly privileged users to help them solve system problems or if an unrecoverable error occurs during normal system operation.

There is no way to predict the contents of memory at the moment a system dump is recorded. The dump may contain clear-text passwords, private encryption keys, user data, or other material that your organization considers to be sensitive or confidential in nature. Therefore, take great care that only authorized personnel handle the dumps. What's more, do not send a dump to anyone outside your organization unless you know that the recipient is authorized to handle such data.

Privileged Users Must Be Trustworthy

Privileged users have access to commands that can violate the security policy of your configuration. Privileged users can enter commands that act directly on objects, and bypass the system's audit and control mechanisms. One command that illustrates this problem is the STORE HOST command.

The CP STORE HOST command allows a class C user to alter any memory location in the z/VM partition. This ability to alter memory used by CP makes it possible for the class C user to negate or bypass the security functionality of the system. Therefore, select only the most trustworthy users for privilege class C.

To avoid possible problems, limit the number of privileged users. Then specify which (if any) can use the STORE HOST command (or any other privileged command that you wish to control access to). To do this, take the following steps:

1. Verify that STORE.C is being controlled in the VMXEVENT profile (it is by default).
2. Activate the VMCMD class.
3. Create a profile, called STORE.C, and grant access to only those you chose.

For more information on protecting CP commands and DIAGNOSE codes with RACF, see *z/VM: RACF Security Server Security Administrator's Guide*.

Note:

The next few items apply to LSM. If this is not appropriate to your system, please go directly to “Administrative Requirements for RACF” on page 34.

Global Access Checking Bypasses MAC and DAC

LSM_Begin

Attention: Objects in the GAC table and minidisks in the global minidisk table are not subject to MAC, DAC, or RACF auditing. (Although objects in the GAC table can be audited using the VMXEVENT auditing for the LINK command.)

Generally, there are two sources of performance problems in an OSPP-compliant system:

- The human cost of constantly maintaining appropriate SECLABELs for each subject and object
- The system cost of performing MAC, DAC, and auditing.

Indiscriminate use of MAC, DAC, and auditing can significantly increase the amount of time required to process your workload. It is therefore important to plan your processes, your computing system, its subjects, and its objects to minimize use of MAC, DAC, and auditing. Ensure that all public objects are either set up in the global minidisk table or the GAC table.

For additional details, see “Objects in GAC Table and Global Minidisk Table Bypass DAC” on page 35.

MDISK Requests Are Subject to MAC

In an OSPP-compliant system, attempts to access a minidisk with either the MDISK control statement or LINK command are subject to DAC testing by RACF. (For more information, see “LINK and MDISK Requests Are Subject to DAC” on page 28.) In an OSPP-compliant system, attempts to access minidisks with the MDISK control statement are also subject to MAC testing by RACF.

Note: In an OSPP-compliant system, RACF downgrades MDISK requests for MR or WR access if the SECLABEL of the user requesting the link does not equal the SECLABEL of the minidisk. In this case, the user receives read-only access to the minidisk, but only if so authorized.

When this downgrade occurs, RACF generates an audit record with access mode RR, indicating that read-only access was granted. An XX audit record may also be generated by CP.

For additional information on the LINK command, see *z/VM: CP Commands and Utilities Reference*. For additional information on the MDISK directory statement, see *z/VM: CP Planning and Administration*.

The SECLABEL of the Creator of a Logical Device Must Equal That of Any of Its Users or be SYSNONE

Users can use DIAGNOSE code X'7C' to create a logical device, such as a logical terminal. When other users attempt to log on the system using that logical device, their SECLABEL is compared with that of the creator of the device. The creator's SECLABEL must equal that of the other user, or the attempt to use the device fails. If such separation is not required, then SECLABEL SYSNONE may be assigned to the logical device creator.

The VM TCP/IP telnet server (user TCPIP) creates logical devices for TN3270 and TN3270E sessions. Unless multiple instances of TCP/IP are to be provided, it is recommended that user TCPIP be assigned SECLABEL SYSNONE.

All Saved Segments and IMG Files Must Be Redefined

Because a security label of SYSLOW is assigned to non-restricted saved segments and IMG files when they are defined, all NSSs, DCSSs, and IMG files must be deleted and redefined after the OSPP-compliant system has been initialized.

For additional information, see the descriptions of the DEFSEG, DEFSYS, and IMAGELIB commands in the *z/VM: CP Commands and Utilities Reference*.

Considerations for NSSs Defined with the VMGROUP Option

Each NSS defined with the VMGROUP option of the DEFSYS command must also be defined with the RSTD option. RACF protection will then be used to protect use of the NSS. For information on setting up a RACF profile for each NSS, see *z/VM: RACF Security Server Security Administrator's Guide*.

If an NSS has been defined with the VMGROUP option and without the RSTD option, the NSS must be deleted and redefined. For additional information, see the DEFSYS command in the *z/VM: CP Commands and Utilities Reference*.

Objects Created by z/VM Receive a SYSHIGH SECLABEL

The z/VM system occasionally creates objects. Every object created by the system is automatically assigned the SYSHIGH SECLABEL — that is, the most sensitive, restrictive label available. The SYSHIGH SECLABEL combines the system's highest security level with all of the system's security categories. For example, the SYSHIGH SECLABEL is always assigned to system dumps and monitor files.

Note: NLS and IMG files are exceptions to this policy. These files are assigned a SECLABEL of SYSLOW.

Store the Human-Readable Label Table

Every time you initialize z/VM, be certain to run the SECTABLE program. (See “Running the SECTABLE Application” on page 42.) This application stores a copy of the current, human-readable label table in CP memory. For details, see “Storing a Copy of the Human-Readable Label Table” on page 41.

Applying SECLABELs to Every Imported Object

Whenever an object is imported into your system, you must assume that it does not have a proper security label. This assumption must persist, even though the object may have a SECLABEL from another system. (There is no reason to assume that such a SECLABEL is valid in your system.)

Thus, the OSPP security policy requires you to handle the importation of every object in the following way:

1. Assign a temporary SECLABEL to the object, allowing only someone with system administrator authority to access it.

2. Examine the object and analyze its significance to the security of your system.
3. Re-assign to the object, based upon this analysis, an appropriate SECLABEL. See *z/VM: RACF Security Server Security Administrator's Guide* for additional information.

Verify SECLABELs Accompanying Data Exported from Your System

Your system contains both single-level devices and multi-level devices, and each has implications in the export of data from your system.

A single-level device is one that handles data of only one particular security label. The SECLABEL takes effect or is changed either by an administrative act or during log on. There are many examples of single level devices, such as printers, terminals, and guest LANs.

A multi-level device is one that handles data associated with any SECLABEL. The only multi-level devices are DASD volumes. These devices may contain data from multiple sources, each with a different SECLABEL. For example, a single DASD volume often contains multiple minidisks, each possibly having a different SECLABEL.

This arrangement affects the export of data outside the system, such as when performing a system backup.

Unlabeled Spool Files Are Not Accessible in an OSPP-Compliant System

All objects and users in an OSPP-compliant system MUST be assigned an appropriate SECLABEL. If a spool file is introduced into the system without a SECLABEL (using SPXTAPE LOAD), the system makes it inaccessible by anyone. In such a case, it is up to the system administrator to give the spool file an appropriate SECLABEL using the CHANGE command. See "The CP CHANGE Command" on page 45.

TLS Connections Produce Unique Audit Records

If auditing is enabled for TLS connections, either via DTCPARMS inclusion of TRACE CONNECTIONS NODATA for the TLS Server or by issuance of the SSLADMIN TRACE CONNECTIONS command, an audit record is generated whenever a connection is attempted to the z/VM system. This data is recorded in the spool area of the TLS worker machine associated with the connection request, and it will list the IP address, domain name, certificate's distinguished name, timestamp, and connection attempt result associated with the transmission.

This data must be gathered manually by the issuance of the SSLADMIN LOG command from an authorized z/VM userid identified to the TLS server by update to the ADMIN_ID_LIST field in the DTCPARMS file. SSLADMIN LOG spools the consoles of the TLS server machine(s) to a designated virtual machine reader. Reader files related to TLS auditing, like all audit records, must be transferred off-platform for sake of analysis or storage. Refer to "Transfer of Audit Records" on page 36 for more information about how to move security-relevant data off-platform.

Note that, per the following section, transferring spool files may produce unique audit records inside of RACF.

Handling of Random Number Generation and Validation of Entropy

Random Number Generation (RNG) in z/VM is handled at the hardware level, via a special instruction set onto the CPUs of IBM Z hardware. Validating the installation of these facilities can be accomplished via issuance of the CP command QUERY CRYPTO (Class A). This will also provide details regarding specialty cryptographic hardware which would fall outside the boundaries of z/VM's Common Criteria evaluations. Note that statements regarding entropy for z/VM are only valid when running on IBM Z z14 hardware or later, as previous generations of the hardware crypto processing only supported Pseudo-Random Number Generation on-chip.

Validating the entropy used by the z/VM TLS Server requires specific instructions, as it involves running traces against the underlying cryptographic library inside the instantiation of the z/VM TLS Server. The entropy pool's seeding, creation, and successful implementation can be viewed by including a GSKTRACE statement inside the DTCPARMS configuration for the TLS Server. Specifically, one would add the following line to the end of the configuration specified in “Required VMSSL Command Operands” on page 17, second configuration:

```
GSKTRACE 015
```

Note that enabling and disabling GSKTRACE can only be done via the configuration file, and is static; it cannot be disabled once initialized without bringing down the TLS Server. Similarly, the resultant GSKTRACE produced can only be gathered by stopping and restarting the TLS Server.

The instructions for gathering a GSKTRACE are documented on the z/VM web page and can be found at: System SSL (GSKTRACE) Tracing Information (https://www.vm.ibm.com/related/tcpip/tcsslgkt.html).

Once the GSKTRACE file has been processed, it must be transferred off-platform for sake of analysis or storage. Refer to “Transfer of Audit Records” on page 36 for more information on how to move security-relevant data off-platform.

Transferring Spool Files Produce Unique Audit Records

If auditing is enabled for the TRANSFER command, an audit record is generated whenever a user enters the TRANSFER command. When the spool file is transferred from one unit record device to another, that event is audited, too. When auditing is enabled for the TRANSFER command, the following commands and DIAGNOSE code are also audited:

- CHANGE TO
- CLOSE TO
- SPOOL FOR
- SPOOL TO
- TRSAVE TO
- VMDUMP TO
- DIAGNOSE code X'94' with the TO parameter.

See Figure 4 on page 33 and Figure 5 on page 33 for examples of the format of each of these audit records.

```
                                                             E
                                                             V  Q
                                                             E  U
                          *JOB/USER  *STEP/    --TERMINAL--  N  A
      DATE    TIME   SYSID   NAME     GROUP       ID    LVL  T  L
     92.323 09:12:17 VMSP   USERG                         0  2  0

     JOBID=(USERG 00.000 00:00:00),USERDATA=()
     AUTH=(NORMAL),REASON=(VMAUDIT)
     VMXEVENT=TRANSFER     USERG    0037 TO PIERSON -,RESOURCE SECLABEL=SECL3
```

Figure 4. An example of an OSPP audit record for the TRANSFER command on an LSM system.

```
                                                            E
                                                             V  Q
                                                             E  U
                          *JOB/USER  *STEP/    --TERMINAL--  N  A
      DATE    TIME   SYSID   NAME     GROUP       ID    LVL  T  L
     92.323 09:12:17 VMSP   USERG                         0  2  0

     JOBID=(USERG 00.000 00:00:00),USERDATA=()
     AUTH=(NORMAL),REASON=(VMAUDIT)
     VMXEVENT=TRANSFER     0012 SFBSTART= 001870,RESOURCE SECLABEL=SECL3
```

Figure 5. An example of an OSPP audit record for the transfer of a spool file.

Note: The format of these audit records is significantly different on systems that do *not* use LSM. See "Security-Relevant Events Can Produce Unique Audit Records" on page 29.

Do Not Include Any Sensitive or Classified Data in Broadcast Messages

If you issue the privileged CP MESSAGE, MSGNOH, or WARNING command with the ALL, ALLSBCS, or ALLDBCS operands, be certain that the message text contains no sensitive or classified data. These commands are not subject to MAC checking. Therefore, it is possible for the message that you send to appear at an unattended terminal console, or at a console not logged on, but whose Enter or Clear key has been pressed.

Messages and warnings sent to and from the system operator are not subject to MAC checking. Therefore, message text sent to or from the system operator MUST NOT contain sensitive or classified data.

TAG Commands Are Subject to MAC

TAG commands with the FILE parameter cause CP to call RACF for a MAC check.

Control of Secondary Users and Observers with MAC

Use of the SET SECUSER or SET OBSERVER commands will cause CP to call RACF for a MAC check. Similarly, if console access is granted via the user directory, MAC checks will be called. These commands enable either write or read access to the console of another virtual machine. Because either virtual machine may contain sensitive information, it must respect security label boundaries.

LSM_End

Administrative Requirements for RACF

Use of Multiple RACF Service Machines

RACF offers an environment in which several RACF service machines can operate in one configuration simultaneously. In a multiple RACF service machine environment, users are assigned to one of several RACF service machines when they log on. Usually, all authorization requests made on the user's behalf are processed by the same RACF service machine to which the user was originally assigned. There are three exceptions to this:

- If the RACF service machine to which the user was originally assigned becomes unavailable, another service machine takes its place.
- If a privileged user (a trusted server, for example) enters a RACROUTE request, they must specify which RACF service machine is to handle the request in the RACF SERVMACH file.
- If the user addresses a RACF command to a specific RACF service machine using RAC.

The database can be shared among more than one RACF service machine if it is stored on an extended count-key-data (ECKD) DASD. It cannot be shared if it is stored on FBA or SCSI DASD.

For additional information, see *z/VM: RACF Security Server System Programmer's Guide*.

Synchronize RACF Operations Across Multiple Service VMs

If an installation is running with multiple servers, it is important to keep certain RACF options synchronized among the servers. For example, profiles within given resource classes can be read from the RACF database into the memory of the service virtual machine to improve performance. This is accomplished through the SETROPTS RACLIST(class_name) command. If the SETROPTS RACLIST(class_name) REFRESH command is issued against that class, the server processing the command refreshes the profiles in memory with current copies from the RACF database. These copies may be different, which would cause a disparity between the access/auditing decisions made by that server and any other server that had previously RACLISTed the class in question. To avoid these types of situations, an installation must ensure that such operations are kept in synchronization across all the

RACF servers. This consideration applies to the RVARY command, and to the RACLIST, RACLIST REFRESH, GENERIC REFRESH, and GLOBAL REFRESH operands of the SETROPTS command.

Attention: These items, which affect the in-memory profiles, should not be modified during periods of heavy activity, as they result in a timing gap in access and audit requests. When changes are necessary, a time should be chosen that minimizes the period of time the RACF servers are not synchronized. If used only for performance reasons, it may be more appropriate to *not* RACLIST a given class.

The RAC EXEC can be used to direct a RACF command to a specific service machine (RAC defaults to use the RACF service machine that was initially associated with the command issuer at LOGON). Note that RAC is the only method in which to accomplish this in a multiple server environment; the RACF command session may not be used. An installation can accomplish this through RAC by setting the global variable $RAC_SRV to the name of the server a particular RACF command is to be directed to. For more information, see the description of the RAC command in the *z/VM: RACF Security Server Command Language Reference*.

For additional information on initializing and using multiple RACF servers, see *z/VM: RACF Security Server System Programmer's Guide*.

Objects in GAC Table and Global Minidisk Table Bypass DAC

Global access checking (GAC) is the test performed by RACF to determine whether a subject should have access to an object and, if so, what type of access. GAC checks a table that lists a group of objects. For each object in the table, there is a mapping that describes the type of access permitted to it, by any subject. That is, each object in the GAC table grants a certain level of access to any and all subjects that request access. If the object appears in the GAC table, the subject immediately receives the specified level of access. To define an object to the GAC table, see *z/VM: RACF Security Server Security Administrator's Guide*. GAC is the first test performed for all objects except minidisks.

The global minidisk table identifies the minidisks in your organization which are considered public. For additional details on this table, see "Public Objects" on page 6. For minidisks, a check of the global minidisk table is the first test completed.

Although identifying objects in the GAC table and global minidisk table reduces RACF overhead, it can also compromise security if an installation handles it improperly. Each object listed must be a public object containing data that is not sensitive. That is, all objects must be READ-ONLY, and there must be no need to audit them.

Attention: Objects in the GAC table and minidisks in the global minidisk table are not subject to DAC or RACF auditing. (Although objects in the GAC table can be audited using the VMXEVENT auditing for the LINK command.)

Performance Considerations

The performance of your system can be improved by copying generic profiles from the RACF database into memory. This is particularly beneficial when used for public objects that are accessed frequently. To activate the GENLIST facility, a user with the SPECIAL attribute enters the following SETROPTS command:

```
SETROPTS GENLIST(class-name)
```

For additional information and specific recommendations, see *z/VM: RACF Security Server System Programmer's Guide*.

Maintain UACC(NONE) in RACF Profiles

Universal access authority (UACC) is the access authority that a user or group receives by default when not explicitly granted access to a particular object. UACC(NONE) must be maintained throughout z/VM for every object. That is, no subject can gain access to an object unless it is explicitly granted. (The exception, of course, is any public object, to which anyone can get READ-ONLY access through the GAC or the global minidisk table.) There are two things you must do to ensure this:

- Set all RACF resource profiles (except those of public objects) to UACC(NONE)
- Specify UACC(READ) for all public objects.

Audit the Use of RACF Privilege

While it is not strictly a Common Criteria security criterion, it may be helpful to the system auditor to keep track of how RACF privilege is used. The auditor may be especially interested in:

- A record of RACF command violations
- An audit of the actions of RACF SPECIAL users
- An audit of the actions of users with the RACF OPERATIONS attribute.

Thus, an administrator with the RACF AUDITOR attribute should enter the following command to RACF:

```
RAC SETROPTS CMDVIOL SAUDIT OPERAUDIT
```

The RACF SETRACF Command Is Always Audited

The RACF SETRACF command activates or deactivates RACF protection over your z/VM configuration. Any administrator can enter the SETRACF command, but only from a RACF service machine.

Because this command has great significance for the security of your system, RACF automatically audits the SETRACF command.

Generating Audit Reports

The system auditor can generate reports to verify that the security policy of the installation is being maintained. RACF provides the report writer function to generate such reports.

The report writer function of RACF lists information contained in the SMF records according to the options the user specifies. These options allow the flexibility to tailor reports to meet the needs of a particular installation. The RACF report writer lets you select specific SMF records, to specify selection criteria related to particular RACF events, to list those SMF records that meet the selection criteria, and to summarize the information obtained from the selected SMF records.

See the *z/VM: RACF Security Server Auditor's Guide* for additional information on using the RACF report writer.

Use of Read-Only Audit

A new RACF user role, ROAUDIT, exists to enable auditors to view audit reports without the capacity to modify them or change audit settings. This user role should be installed based upon human job authorities and need-to-know as appropriate.

Transfer of Audit Records

In addition to maintaining a robust auditing policy around security events, care must be taken to transfer audit records off-platform for sake of analysis or storage. The specifics of timing or frequency are not mandated by the Common Criteria; however, it is recommended that events be offloaded on a regular basis for analysis, either by hand or via the Security Intelligence Event Monitoring (SIEM) platform of your choice. The rationale for this is that an audit record unchecked is equivalent to not having generated an audit record at all, and may constitute a failure to recognize a malicious security event.

Transfer of audit records for archival purposes is also pertinent, in case of broader auditing requirements. Consult local security policy to determine the length of time for which audit records must be maintained.

In order to transfer audit records, use appropriate communication channels to transmit to the destination system of your choice. The example automation below uses FTPS (FTP over TLS), as the z/VM evaluated configuration makes extensive use of TLS for encryption of data in flight. This should be placed on the RACFSMF userid, which is the virtual machine used by the ESM to generate SMF records as part of the auditing process. Note that FTPS should only be executed after auditing records have been received from the ESM work disks.

The FTP command allows you to transfer files between your local host and a foreign TCP/IP host. See the chapter titled "Transferring Files Using FTP" in *z/VM: TCP/IP User's Guide*.

Example

This FTP command with the SECURE option establishes a secure connection. To transfer files to a foreign host, a working directory must be established for which you have at least write access.

```
cp link tcpmaint 592 592 rr      (Link the minidisk that has the FTP command.)
access 592 b                     (Access as filemode b.)
FTP  ipaddr ( SECURE             (Specify the IP address of the foreign host.)
```

Enter the userid and password for the foreign host.

```
CD filepoolid:userid             (Change to your working directory; this could also be
userid.vaddr.)
MODE B                           (Set block mode.)
TYPE E                           (Set the transfer as EBCDIC.)
PUT  filename.filetype.filemode  (Transfer the SMF DATA file from the local host to the
foreign host.)
QUIT                             (Disconnect from the foreign host and end FTP.)
```

RACF Considerations in an SSI Environment

A z/VM single system image (SSI) cluster is a multisystem environment in which the z/VM member systems can be managed as a single resource pool and running virtual servers (guests) can be relocated from one member to another. For more information about the SSI environment and setting up SSI clusters, see *z/VM: CP Planning and Administration*.

Shared RACF Database

When operating in an SSI environment, all member systems of a cluster must share a common RACFVM database. It must be stored on a full-pack ECKD minidisk; it cannot be shared if it is stored on an FBA or SCSI device. For more information, see *z/VM: RACF Security Server System Programmer's Guide*.

SETROPTS, RVARY, and SETEVENT Commands

If you issue the SETROPTS command with any operand that changes the RACF database or issue the SETROPTS REFRESH command or issue the SETEVENT command, the command is automatically propagated to all RACF servers that run on the same z/VM system, and to other systems in the same SSI cluster as the issuing system. SETROPTS LIST is the only SETROPTS command that is not propagated.

On a system outside an SSI cluster, the action is not propagated to other systems that share the RACF database. You must issue the command separately for each system or restart the RACF servers on the other system or IPL the other system.

Attention: These items, which affect the in-memory profiles, should not be modified during periods of heavy activity, as they could result in a timing gap in access and audit requests. When changes are necessary, a time should be chosen that will minimize the period in which the RACF servers are not synchronized. If used only for performance reasons, it may be more appropriate to not RACLIST a given class.

Multi-factor Authentication Must be used for Human Users

If available, multi-factor authentication should be enabled for administrators of the z/VM system. In this case, MFA must be established for virtual machines which correspond to human users of the system, rather than "technical users" or "service virtual machines" that represent a privileged operational context that does not allow for direct human intervention.

- RACF must be set to enable MFA.

  The RACF Security Server shall enable the capacity for MFA, assuming that the IBM Z Multi-factor Authentication product is somewhere within the z/VM Single System Image cluster. Connection to the MFA server is controlled by the MFA CONTROL file.
- Connections to MFA must be secure.

  Update appropriate PORT settings in the PROFILE TCPIP to point RACF through the z/VM TCP/IP stack in order to communicate with IBM Z MFA.
- Users which do not require MFA should specify NOMFA.

  This includes AUTOONLY virtual machines and PROTECTED virtual machines, which should be marked as NOPASS NOPHRASE NOMFA.
- Enable administrators for MFA access, and determine if Password Fallback is allowed. An administrator or system programmer should be modified in RACF with the MFA option on ADDUSER or ALTUSER.

  A Password Fallback option (PWFALLBACK) can be granted if this particular human should be allowed to access the system with a traditional RACF password or password phrase. This is useful in case of disaster recovery scenarios, or cases when the MFA server is not available. In this case, normal password rules under the Common Criteria shall apply to this factor.

  Use of PWFALLBACK is both audited in RACF, and a message is sent to the System Operator to alert administrators and potentially automated processes that this capacity was used.
- Configure factors appropriate for your environment.

  The Common Criteria does not mandate a particular set of factors, save that there should be a minimum of two (2) factors, and they should be of a combination of known information, objects held, and biometrics ("what you have, what you know, and/or what you are").
- The Linux on IBM Z guest on which the MFA Server runs should be configured in accordance with any Linux on IBM Z Common Criteria guidance as appropriate.

Chapter 4. Additional Topics for LSM

LSM_Begin

This chapter describes CP printer support and other topics that have implications in a compliant z/VM system using LSM.

CP Printer Support

CP printer support is the basic printing system support that comes with every z/VM system. Through this support, CP directly controls one or more printers physically attached to the computer. CP printer support meets Common Criteria only with human intervention (for more specific details, see "Human Intervention Needed to Meet Common Criteria" on page 39), and the following two security enhancements:

- Identification labels for the header and trailer pages. See "Human-Readable Labels" on page 40.
- Random security numbers for the header and trailer pages. See "Random Security Numbers for Print Jobs" on page 43.

Human Intervention Needed to Meet Common Criteria

Because CP printer support does not have automatic data page labeling, a human must manually ensure that the security label is placed on the bottom and top of each page. For example, if a SYSHIGH SECLABEL is needed on each page of output, the printer operator must:

- Stop the printer (if it was running)
- Load the printer with paper that has the human-readable version of the SYSHIGH label on the top and bottom of every page
- Start the printer at the SYSHIGH SECLABEL until the desired document is printed.

As long as these rules are followed, CP printer support meets the OSPP criteria.

z/VM supports single-level printers, which cannot print documents unless they bear one particular security label. Only after the operator stops, changes the pre-printed forms (pre-printed with the human-readable label), drains, and restarts the printer with a different SECLABEL can it print documents with another security label. It is the responsibility of the printer operator to verify that the SECLABEL and the pre-printed label match.

MAC Protection of CP Printers

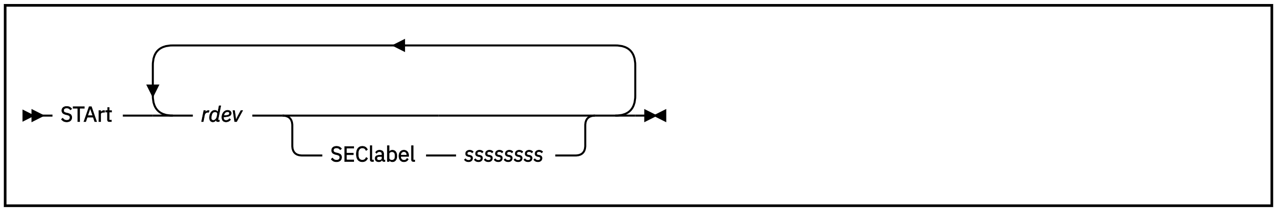
MAC protection for all CP printers is an OSPP requirement. To bring a CP printer under MAC protection, do the following after installation or initialization of your system, or of a new printer.

Use the CP START command to declare the security label of each printer. This security label will remain in affect until it is changed with the CP START command or the system is restarted.

Note: Be certain that the security label you specify with the CP START command is a valid SECLABEL in the printer's RACF profile. Also, remember that the use of the SECLABEL NONE is not recommended. A SECLABEL of NONE is assigned by CP when the printer is initialized. No files are allowed to be printed until the printer is STARTed with a valid SECLABEL.

Use the CP START command to change a printer's security label. A partial diagram of the format of this command follows. For complete information, see the *z/VM: CP Commands and Utilities Reference*.

© Copyright IBM Corp. 2005, 2024



where:

SEClabel *ssssssss*
specifies the security label to be associated with the printer. That is, this printer can accept and print a job only if the job bears this SECLABEL. If no printer with the appropriate characteristics is available, the printer spool file waits until one becomes available.

Note:

1. The NOSEP option is not allowed when security label checking is enabled. If you include this option, you will receive an error message.
2. The SECLABEL option is valid only if security label checking is enabled. (To activate security label checking, see step "11" on page 24.)

In a compliant system, you may see this response:

```
654E   SECLABEL missing or invalid
```

In this case, you should reissue the command with a valid 1- to 8-character SECLABEL.

Human-Readable Labels

The header and trailer pages bear a human-readable label associated with the SECLABEL under which the material is printed.

To illustrate, let's add a fourth column to Table 1 on page 11:

Table 3. A hypothetical mapping of SECLABEL character strings to security levels, categories, and indentification labels

SECLABEL Character String	The Security Level	The Security Categories	Human-Readable Label
SECL1	TOPSEC	PROJA PROJB PROJC	"This material is TOP SECRET and to be seen only by appropriately authorized members of PROJECTS A, B, and C."
SECL2	SECRET	PROJC PROJD PROJE	"This material is SECRET and to be seen only by appropriately authorized members of PROJECTS C, D, and E."
SECL3	CONF	PROJB	"This material is CONFIDENTIAL and to be seen only by appropriately authorized members of PROJECT B."
SECL4	CONF	PROJD PROJE	"This material is CONFIDENTIAL and to be seen only by appropriately authorized members of PROJECTS D and E."

Table 3. A hypothetical mapping of SECLABEL character strings to security levels, categories, and indentification labels (continued)

SECLABEL Character String	The Security Level	The Security Categories	Human-Readable Label
SECL5	CONF	PROJE	“This material is CONFIDENTIAL and to be seen only by appropriately authorized members of PROJECT E.”

Map Security Label Character Strings to Human-Readable Labels

To map security label character strings with human-readable labels, the administrator has three tasks:

1. “Creating the Human-Readable Label Table” on page 41.
2. “Storing a Copy of the Human-Readable Label Table” on page 41.
3. “Updating the Human-Readable Label Table” on page 42.

Creating the Human-Readable Label Table

The human-readable label table contains the mapping between the SECLABEL character strings and the human-readable labels. To create this table, proceed as follows:

1. Create a file named SECTABLE FILE. It must be of variable length format with a logical record length from 10 to 141. As you develop this file, allow it to grow no larger than 65,536 bytes (64KB).
2. Create one record for each SECLABEL and its associated human-readable label. The format for each record in SECTABLE FILE is as follows:

Table 4. Record format for SECTABLE FILE

Column	Content
1 - 8	SECLABEL character string
9	Required blank space
10 - 141	Human-readable label (1 to 132 characters long)

3. Store SECTABLE FILE on AUTOLOG2's 191 disk.

Your human-readable label table is now ready to be stored for use by CP.

Storing a Copy of the Human-Readable Label Table

The SECTABLE application stores an up-to-date, working copy of your human-readable label table for use by CP. To store a copy of the human-readable label table in CP memory, do the following:

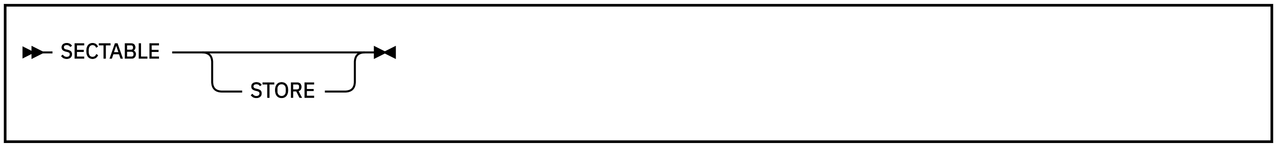
1. Place the system in the tranquil state by issuing the following RACF command:

```
RAC SETROPTS MLQUIET
```

2. Run the SECTABLE application. See “Running the SECTABLE Application” on page 42.
3. Restore the system to usual running mode by issuing the following RACF command:

```
RAC SETROPTS NOMLQUIET
```

Running the SECTABLE Application



where:

STORE

alters the human-readable text associated with each SECLABEL listed in the file SECTABLE FILE. The first copy of SECTABLE FILE found in the CMS file search order will be used.

To use the STORE operand, you must have READ access to the DIAG0A0.HRTSTORE profile in the VMCMD class. If protection for DIAGNOSE X'A0' has been turned off, then you must have class A or B privilege.

If you omit the STORE operand, no special privileges are required as the file will only be checked for correct syntax.

Note:

1. SECTABLE STORE must be run each time the system is IPLed. Alter the PROFILE EXEC for AUTOLOG2 to issue the SECTABLE STORE command before any other service machines or system printers are started.

   When running an SSI cluster, updates should be made to each member's AUTOLOG2 PROFILE EXEC.
2. A system printer has a default security label of NONE and will not print until SECTABLE STORE has been issued and a valid SECLABEL has been specified on the CP START command. The SECLABEL must be listed in SECTABLE FILE.
3. For more information on RACF authorization for DIAG0A0.HRTSTORE, see *z/VM: RACF Security Server Security Administrator's Guide*.

Messages:

```
HCP8601I      All SECTABLE file records were found to be valid.
HCP8602I      SECLABEL/HRL correlation table has been successfully stored.
HCP8603E      Invalid operand specification on SECTABLE invocation.
HCP8604E      Error from CMS macro name with return code retcode.
HCP8605E      SECTABLE FILE must have LRECL not < 10, LRECL not > 141, and
              RECFM = V.
HCP8606E      SECTABLE FILE is too large - CP virtual buffer will be > 64K BYTES.
HCP8607E      Record n causes CP virtual buffer to overflow 64K bytes.
HCP8608E      The following represent invalid SECTABLE FILE records:
HCP8609E      A total of n records were found to be invalid.
HCP8610E      Condition code of n upon return from DIAGNOSE code X'A0'
              subcode X'34' processing.
HCP8611T      Severe error occurred during DIAGNOSE X'A0' subcode X'34'
              processing.
```

When this function is complete, register 15 contains one of these return codes:

```
2    The SECTABLE application program was invoked incorrectly.
4    An error occurred in a CMS macro.
6    The logical record length and/or the record format of SECTABLE FILE were
     invalid.
8    SECTABLE FILE is too large.
10   Invalid SECTABLE FILE records were found.
12   The condition code from DIAGNOSE X'A0' subcode X'34' indicates an error.
```

Updating the Human-Readable Label Table

At some point, you'll want to update the human-readable label table by adding a new SECLABEL or by modifying an existing one. This is an important task, because each SECLABEL declared in RACF MUST be recorded in the human-readable label table. If not defined, CP will print the SECLABEL value instead of the human-readable equivalent. Also, if the SECLABELs declared in RACF are not synchronized with the SECLABELs in SECTABLE FILE, the OSPP security policy will be violated.

To update the human-readable table, proceed as follows:

1. Drain all CP printers.
2. Modify the SECTABLE FILE, making certain that each record in the file conforms to the formatting requirements described in Table 4 on page 41.
3. Give CP its copy of the new file by following the procedure under "Storing a Copy of the Human-Readable Label Table" on page 41.

Random Security Numbers for Print Jobs

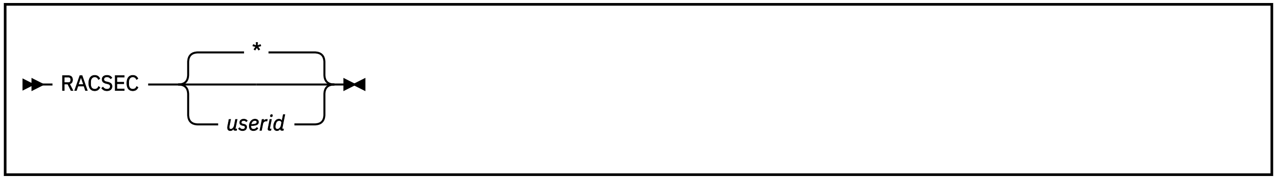
Header and trailer pages must also bear an identical, randomly-generated security number.

This number makes it possible for printer operators to detect any attempt to deceive them into misdirecting a print-out. The same random number must appear on both the header and trailer pages; otherwise, the header and trailer pages are invalid. It is highly unlikely that any malicious parties could accurately guess the random number associated with a particular print job. That means they could not generate a convincing header or trailer page that would fool the printer operator into directing the print-out to an unauthorized destination. If the numbers do not match, the printer operator must retain the material for examination by the system administrator. Such material MUST NOT be distributed to any user, and MUST be retained by the printer operator for examination by the system administrator.

The RACSEC Program (Querying a User's Current SECLABEL)

The RACSEC program is provided to query a user's current security label. This is a useful function for problem determination. Users may be given access to any number of security labels, but may have only one security label active at any given time. As a result, the user will be denied access to data protected by a security label other than the one specified (or defaulted) when the user logged into the system. In the event that the user attempts to access some data and is denied, the RACSEC program allows the user, or an administrator, to quickly determine the user's current security label. If it is determined that the user is at an incorrect security label, the user can log off and log back on at the required security label. (See "The LOGON Command" on page 44 for information on logging on under a specific SECLABEL.)

To run RACSEC, you simply provide a user ID as follows:



where:

*****
indicates that you wish to query your own security label.

userid
identifies the user whose security label you wish to query. You must have privilege class A, or B, or READ access to the DIAG0A0.QUERYSEC profile, to use this option.

Note:

1. RACSEC may be run with no parameters, or with * to query your own current security label. To query another user's security label you need either READ access to the DIAG0A0.QUERYSEC profile, or if that profile is not being used, you must have A or B privilege. If you do not have either of these, then invoking RACSEC will result in a privileged operation exception if you are querying another user's security label.
2. For additional information, see *z/VM: RACF Security Server Security Administrator's Guide*.

A successful response from the RACSEC program appears as follows:

```
RACSEC004I    Security label for user userid is seclabel.
```

Unsuccessful responses appear as follows:

```
RACSEC001A    The RACSEC EXEC could not locate the RPIQSEC MODULE on any disk.
RACSEC002I    Userid userid is not currently logged on, or does not have a
              security label.
RACSEC003A    RACF is currently unable to return the security label.
```

For additional information, see *z/VM: RACF Security Server Messages and Codes*.

The LOGON Command

Specifying **SEClabel *ssssssss*** on the LOGON command (where *ssssssss* is the 1- to 8-character SECLABEL character string), lets you define the security label that will govern your session. RACF tests to see if you are authorized to work under the security label you select. The SECLABEL option is only allowed when security label checking is enabled. (To activate security label checking, see step "11" on page 24.)

If you omit the SECLABEL option from the LOGON command, the system consults your RACF user profile to obtain your default SECLABEL.

Messages:

```
050E         LOGON unsuccessful--incorrect userid and/or password
264I         One or more options are ignored during reconnect processing - option(s)
```

For the complete command description for LOGON, see *z/VM: CP Commands and Utilities Reference*.

The CP QUERY READER/PRINTER/PUNCH Command

If you are a privilege class D user, you can examine the SECLABELs of spool files in any user's virtual machine by specifying the **SEClabel** option on the CP QUERY READER/PRINTER/PUNCH command. For more information, see the *z/VM: CP Commands and Utilities Reference*.

Generally, this is a prelude to changing the SECLABEL of one or more of these files, using the CP CHANGE command. See "The CP CHANGE Command" on page 45. (Class G users can also use this command to change their own spool files.)

Note:

1. RACF must be installed and security label checking must be enabled to use the SECLABEL option.
2. When the SECLABEL option is included on QUERY READER, QUERY PRINTER, or QUERY PUNCH, the system adds an extra column labeled SECLABEL to accommodate the security label for each spool file. (For class G users, the KEEP and MSG columns are replaced by the SECLABEL.)
3. To query a spool file, the user's SECLABEL must dominate that of the file. That is, users must be authorized to at least read the file. If users are so qualified, that means they are also qualified to unrestricted information about the spool file. Here is an example of the unrestricted response such a user might receive to a QUERY command:

   ```
   ORIGINID FILE CLASS RECORDS  CPY HOLD FORM     DEST     SECLABEL
   ONEILD   1914 A PUN 00000567 001 NONE STANDARD OFF      SEC1
   ```

4. If, however, the user is not authorized to at least read the spool file, the system prevents the user from seeing certain sensitive fields in the QUERY command response. Notice, in these examples, that the system masks these fields with asterisks.

   First, a response to a QUERY READER command without SECLABEL option:

   ```
   ORIGINID FILE CLASS RECORDS  CPY HOLD FORM     DEST     KEEP MSG
   TONYN    0012 A PUN ******** *** NONE ******** ******** **** ****
   ```

   Next, a response to a QUERY READER command with SECLABEL option:

   ```
   ORIGINID FILE CLASS RECORDS  CPY HOLD FORM     DEST      SECLABEL
   PIERSON  1914 A PUN ******** *** NONE ******** ********  ********
   ```

Note: If the spool file does not have a security label assigned, the SECLABEL field contains the word NONE.

5. You can PURGE any of your spool files, regardless of the SECLABEL associated with the spool file.
6. You cannot include the SECLABEL option of the CP QUERY command with the ALL, EXP, or PSF option. They are mutually exclusive.

The CP CHANGE Command

The Common Criteria security policy forbids access to any subject or object in the system that does not have a security label. One sort of object, a spool file, may be imported from another system. This means that it may not have a valid security label assigned to it.

Specifying **SEClabel *ssssssss*** on the CP CHANGE command (where *ssssssss* is the 1- to 8-character SECLABEL character string), lets the spooling operator (privilege class D) change the SECLABEL value or add one to any spool file in the system.

Note:

1. The SECLABEL option is valid only when security label checking is enabled and the system is in a tranquil state, or when the user is exempt from security label checking. (To activate security label checking, see step “11” on page 24.)
2. To place the system in a tranquil state, enter the following RACF command:

   ```
   RAC SETROPTS MLQUIET
   ```

   Then, if the spool file is currently in use, perform your installation's procedure to obtain control over it. (That is, force all non-trusted users off the system, force off the user who has control of the spool file, or whatever your administrator calls for.)

   Later, to restore the system to usual running mode, enter the following RACF command:

   ```
   RAC SETROPTS NOMLQUIET
   ```

3. To exempt a user, the security administrator creates an individual VM event profile with a member list that specifies that all controllable events are not to be controlled. For additional information, see the *z/VM: RACF Security Server Security Administrator's Guide*.
4. Each spool file changed through any CHANGE command receives a separate RACF call, for ease of audit and control.

Messages:

```
356E          Access denied; User userid file spoolid not
              {changed|transferred|printed}
654E          SECLABEL missing or invalid
```

For the complete command description for CP CHANGE, see the *z/VM: CP Commands and Utilities Reference*.

DIAGNOSE Code X'BC'

Unless a user's SECLABEL dominates that of a spool file, they cannot read it. In fact, if a user tries to open a spool file, using DIAGNOSE X'BC', and the user is not authorized to read the file, then the MAC check fails and the system withholds most information about the spool file. That is, if the user's SECLABEL does not dominate that of the spool file, the system does not fill in all the fields of the user-supplied buffer. The system supplies only the following fields with meaningful data:

USER ID
FILE ID
CLASS
TYPE
STATUS

DATE
TIME

The other fields of the buffer are filled in with asterisks.

Note: In this case, the spool file is not opened but the return code is set to zero.

Application programs may be expecting a return code of zero to indicate that all data is valid and may need to be modified to handle the asterisks.

DIAGNOSE Code X'D4'

Often, one virtual machine is called upon to do work for another virtual machine. Subcode X'04' of DIAGNOSE X'D4' allows a master virtual machine to use a worker virtual machine to perform work under a SECLABEL that is compatible with that of the end-user on whose behalf the work is being done. Thus, any output generated by the alternative worker machine has the same SECLABEL as the work assigned to it.

Note: Any server that issues DIAGNOSE X'D4' must be part of the evaluated configuration.

The register values at entry are as follows:

Rx
The subcode, X'04'.

Ry
The address of a 24-byte parameter list supplied by the server. The format of the parameter list is as follows:

0
DD4PTGT

8
DD4PALT

10
DD4ALTSC

Note:

1. To simultaneously set up an alternative SECLABEL and an alternative user, use DIAGNOSE X'D4' subcode X'04'.
2. To cancel the alternative SECLABEL, call DIAGNOSE X'D4' subcode X'04' with a SECLABEL or alternative user ID of binary zeros in the parameter list.
3. The worker virtual machine acquires the security label specified in DD4ALTSC in the parameter list above.
4. For additional information on DIAGNOSE code X'D4', see *z/VM: CP Programming Services*.

The CMS RDRLIST Command

The appearance of your RDRLIST panel changes when SECLABEL checking is enabled.

In Figure 6 on page 47, notice that some response fields are masked by asterisks. This indicates that the SECLABEL governing your current session does not dominate that of the spool file.

```
 JSMITH   RDRLIST     A0  V 108  Trunc=108 Size=5  Line=1 Col=1 Alt=1
Cmd     Filename Filetype Class User At Node   Hold  Records  Date  Time
        PROJA    PLANS    PUN A TONYN   NODE7  NONE     9410  9/22  3:30:57
        PROJD    PLANS    PUN A PIERSN  NODE7  NONE    11074  9/26  5:35:21
        PROJE    NOTE     PUN A FGREEN  NODE7  NONE       67  9/22  3:30:27
        ******** ******** PUN A MARKMM  NODE7  NONE ********  9/26  5:35:10
        PROJB    MEMO     PUN A PJONES  NODE7  NONE       32  9/12  8:30:21













1= Help     2= Refresh  3= Quit     4= Sort(type)   5= Sort(date) 6= Sort(user)
7= Backward 8= Forward  9= Receive 10=             11= Peek      12= Cursor

====>
                                                              X E D I T  1 File
```

Figure 6. An example of the RDRLIST panel.

LSM_End

Appendix A. Security-Relevant Commands, DIAGNOSE Codes, and System Functions

The following tables present the security-relevant CP commands, DIAGNOSE codes, and system functions.

These tables have several columns:

- The first column lists the command name, DIAGNOSE code, or system function name.
- For the CP Commands and DIAGNOSE Codes tables, the second column shows the operand name or DIAGNOSE subcode.
- The VMXEVENT Member column indicates the profile name within RACF.
- The Class column indicates the CP privilege class of the command.
- The "CC-Secure" and "CC-Secure with LSM" columns indicate the type of protection provided, as related to both the OSPP and to the NIAP VPP. The types of protection available are as follows:
  - Audit – The use of the command can be audited by RACF if designated in the RACF profile for this command.
  - DAC – Command processor calls RACF to verify the authorization for a specific object or action, using access lists.
  - MAC – For LSM only, command processor calls RACF to perform a SECLABEL comparison between a subject and an object. This column lists the type of MAC check (R/O, R/W, or W/O) or "access," which means the user must have read access to the SECLABEL.

For those commands not in the list, there is no need for any type of protection. Some commands have comments describing specific characteristics of the command that make them security relevant in some circumstances.

Security-Relevant CP Commands

Table 5. Security Relevant CP Commands

Command	Operand	VMXEVENT Member	Class	CC-Secure		CC-Secure with LSM		
				Audit	DAC	Audit	DAC	MAC
ATTACH	device	ATTACH		optional	optional	optional	mandatory	R/W
ATTACH	XSTORE	ATTACH		optional	optional	optional	mandatory	R/W
AUTOLOG[4]		AUTOLOG.A, AUTOLOG.B	A,B	optional	no	optional	no	W/O with access
CHANGE		CHANGE.G	G	optional	no	optional	no	W/O
CHANGE	SECLABEL	CHANGE.D	D	optional	no	optional	no	no
CHANGE	TO	CHANGE.G, TRANSFER.G	G	optional	optional	optional	optional	W/O
CLOSE	TO	CLOSE, TRANSFER.G	G	optional	optional	optional	optional	no
COUPLE		COUPLE	G	optional	no	optional	no	R/W
DEFSYS		DEFSYS		optional	no	optional	no	no
DEFSEG		DEFSEG		optional	no	optional	no	no
DIAL		DIAL		no	mandatory[1]	no	mandatory[1]	no
FOR		FOR.C, FOR.G	C,G	optional	optional	optional	optional	R/W
GIVE		GIVE		optional	no	optional	no	no

Table 5. Security Relevant CP Commands (continued)

Command	Operand	VMXEVENT Member	Class	CC-Secure		CC-Secure with LSM		
				Audit	**DAC**	**Audit**	**DAC**	**MAC**
IPL	sysname	IPL		optional	mandatory[2]	optional	mandatory	R/O or R/W
LINK		LINK		optional	mandatory	optional	mandatory	R/O or R/W
LOGOFF		LOGOFF		optional	no	optional	no	no
LOGON[4]	SECLABEL, HERE	LOGON		optional	no	optional	no	access
LOGON	to logical device	LOGON		optional	no	optional	no	R/W[3]
MESSAGE		MESSAGE.ANY	ANY	optional	mandatory[1]	optional	mandatory[1]	W/O
MESSAGE	ALL, ALLDBCS, ALLSBCS	MESSAGE.A, MESSAGE.B	A,B	optional	no	optional	no	no
MSGNOH		MSGNOH	B	optional	no	optional	no	W/O
MSGNOH	ALL, ALLDBCS, ALLSBCS	MSGNOH	B	optional	no	optional	no	no
QUERY	RDR/PRT/PUN	QUERY.READER.G, QUERY.READER.D, QUERY.PRINTER.G QUERY.PRINTER.D, QUERY.PUNCH.G, QUERY.PUNCH.D		optional	no	optional	no	R/O
QUERY	rdev	none		optional	no	optional	no	no
QUERY	TAG	QUERY.TAG		optional	no	optional	no	R/O
QUERY	TRFILES	QUERY.TRFILES.A, QUERY.TRFILES.C, QUERY.TRFILES.D, QUERY.TRFILES.E, QUERY.TRFILES.G		optional	no	optional	no	R/O
RESET	RESERVE	RESET.B		optional	no	optional	no	no
SEND		SEND.C	C	optional	no	optional	no	W/O
SEND[5]		SEND.G	G	optional	no	optional	no	R/W
SET	LOGMSG	SET.LOGMSG	B	optional	no	optional	no	no
SET	OBSERVER	SET.OBSERVER.A, SET.OBSERVER.C, SET.OBSERVER.G,	A,C,G	optional	no	no	no	R/O
SET	PASSWORD	SET.PASSWORD	B	optional	no	optional	no	no
SET	PRIVCLAS	SET.PRIVCLASS.C, SET.PRIVCLASS.ANY	C,ANY	optional	no	optional	no	no
SET	SECUSER	SET.SECUSER.A, SET.SECUSER.C, SET.SECUSER.G	A,C,G	optional	no	no	no	R/W
SMSG		SMSG		optional	no	optional	no	W/O
SPOOL	FOR, TO	SPOOL, TRANSFER.G		optional	optional	optional	optional	no
START	SECLABEL	START.D		optional	no	optional	mandatory	no
STORE	HOST	STORE.C		optional	optional	optional	optional	no
TAG	DEVICE	TAG		optional	optional	optional	optional	no
TAG	FILE	TAG		optional	optional	optional	optional	W/O

Table 5. Security Relevant CP Commands (continued)

Command	**Operand**	**VMXEVENT Member**	**Class**	**CC-Secure**		**CC-Secure with LSM**		
				Audit	**DAC**	**Audit**	**DAC**	**MAC**
TAG	QUERY	QUERY.TAG		optional	no	optional	no	R/O
TRANSFER		TRANSFER.D, TRANSFER.G	D,G	optional	optional	optional	optional	no
TRSAVE	TO	TRSAVE.A, TRSAVE.C, TRANSFER.D		optional	optional	optional	optional	no
TRSOURCE		TRSOURCE		optional	optional	optional	optional	no
TRSOURCE	ENABLE	TRSOURCE		optional	no	optional	mandatory	R/W
UNDIAL		UNDIAL		no	mandatory[1]	no	mandatory[1]	no
VMDUMP	TO	VMDUMP, TRANSFER.G		optional	optional	optional	optional	no
VMRELOCATE		VMRELOCATE	A	optional	no	optional	no	no
WNG		WARNING.A, WARNING.B, WARNING.C	A,B,C	optional	no	optional	no	W/O
WNG	ALL, ALLDBCS, ALLSBCS	WARNING.A, WARNING.B	A,B	optional	no	optional	no	no
XAUTOLOG[4]	ON	XAUTOLOG.A, XAUTOLOG.B	A,B	optional	no	optional	no	W/O
XAUTOLOG[4]		XAUTOLOG.G	G	optional	mandatory	optional	mandatory	W/O

Note:

[1] The DIAL, MESSAGE and UNDIAL command must be disabled prior to LOGON.

[2] This only applies to restricted members.

[3] If logging on from a device that was created with DIAGNOSE X'7C' a R/W MAC will be made to ensure that SECLABEL of the creator of the device and the SECLABEL of the person logging on are equal.

[4] User authentication is performed, including password checking, if necessary.

[5] Although the SEND itself might be considered write-only, a class G SEND command is only permitted if the issuer is a functional secondary user for the target, which requires read-only access. So a class G SEND command requires equivalent seclabels (W/O+R/O).

DIAGNOSE Codes

Programs running in the virtual machine may request services from CP using the DIAGNOSE instruction. The following table discusses the security relevant DIAGNOSE codes.

Table 6. Security Relevant DIAGNOSE Codes

DIAGNOSE	**Subcode**	**VMXEVENT Member**	**Class**	**CC-Secure**		**CC-Secure with LSM**		
				Audit	**DAC**	**Audit**	**DAC**	**MAC**
X'04'		DIAG004	E	optional	no	optional	no	no
X'08'		DIAG008		avoid	no	avoid	no	no
X'14'[1]	0,2C	DIAG014		optional	no	optional	no	R/O
X'14'	4,8,FFE,FFF	DIAG014		optional	no	optional	no	R/O
X'34'[1]		DIAG034		optional	no	optional	no	R/O
X'4C'		DIAG04C		optional	no	optional	no	no
X'64'[2]	0,4,C,10,18	DIAG064		optional	mandatory	optional	mandatory	R/O or R/W
X'68'	2,3,4,5,7,A	DIAG068		optional	no	optional	no	R/O, W/O or R/W

Table 6. Security Relevant DIAGNOSE Codes (continued)

DIAGNOSE	Subcode	VMXEVENT Member	Class	CC-Secure		CC-Secure with LSM		
				Audit	DAC	Audit	DAC	MAC
X'74'		DIAG074	A,B,C, E	optional	no	optional	no	no
X'7C'[3]		DIAG07C		optional	no	optional	no	no
X'84'		DIAG084		optional	no	optional	no	no
X'88'		DIAG088		optional	optional	optional	optional	no
X'90'		DIAG090	E	optional	no	optional	no	no
X'94' with the TO option		DIAG094, TRANSFER.G		optional	optional	optional	optional	no
X'98'		DIAG098		optional	no	optional	no	no
X'A0'	30,34,4[4]	DIAG0A0		optional	optional	optional	optional	no
X'B8'[1]		DIAG0B8		optional	no	optional	no	R/O or W/O
X'BC'		DIAG0BC		optional	no	optional	no	R/O
X'CC'		DIAG0CC		optional	no	optional	no	no
X'D4'		DIAG0D4		optional	optional	optional	optional	access
X'E0'[1]		DIAG0E0		optional	no	optional	no	R/O
X'E4'		DIAG0E4		optional	optional	optional	optional	no
X'FC'		DIAG0FC		optional	no	optional	no	no
X'23C'	3	DIAG23C		optional	no	optional	no	R/O or R/W

Note:

[1] This DIAGNOSE calls the spool file open routine (as for system functions SPF_OPEN or SDF-OPEN).

[2] This only applies to restricted members.

[3] If logging on from a device that was created with DIAGNOSE X'7C' a R/W MAC will be made to ensure that SECLABEL of the creator of the device and the SECLABEL of the person logging on are equal.

[4] User authentication is performed, including password checking, if necessary.

System Functions

Some system functions are protected by RACF. The following table shows the protection available.

Table 7. Security Relevant System Functions

Function	VMXEVENT Member	CC-Secure		CC-Secure with LSM		
		Audit	DAC	Audit	DAC	MAC
APPC connect	APPCCON	optional	no	optional	no	R/W
APPC password validation[1]	APPCPWVL	optional	mandatory	optional	mandatory	access
CP command issued from directory	DIRECTRY_CMD	optional	no	optional	no	no
IUCV connect	IUCVCON	optional	no	optional	no	R/W
Load/find of restricted segment	RSTDSEG	optional	mandatory	optional	mandatory	R/O or R/W
MDISK	MDISK	optional	optional	optional	mandatory	R/O or R/W
Print of spool file	UTLPRINT	optional	no	optional	no	access
Spool file create	SPF_CREATE	optional	no	optional	no	no

Table 7. Security Relevant System Functions (continued)

Function	VMXEVENT Member	CC-Secure		CC-Secure with LSM		
		Audit	DAC	Audit	DAC	MAC
Spool file delete	SPF_DELETE	optional	no	optional	no	no
Spool file open	SPF_OPEN	optional	no	optional	no	R/O
System data file create	SDF_CREATE	optional	no	optional	no	no
System data file delete	SDF_DELETE	optional	no	optional	no	no
System data file open	SDF_OPEN	optional	no	optional	no	R/O
Virtual network sniffer state change	SNIFFER_MODE	optional	mandatory[2]	optional	mandatory[2]	no

Note:

[1] User authentication is performed, including password checking, if necessary.

[2] Authorization to promiscuously sniff traffic on a guest LAN or virtual switch requires CONTROL access to the associated VMLAN resource.

Appendix B. Security Objectives for the IT Environment

The evaluated configuration of z/VM is based on security objectives that must be met by the IT environment in order to achieve and maintain secure operations:

- z/VM administrators must be competent and trustworthy individuals, capable of managing the system and the security of the information it contains.
- Any networked system in which z/VM needs to interact, whether to keep up its proper function or to fulfill any security policy, must be protected from attack and are under the same management domain as z/VM. These other networked systems must be managed according to the same rules and policies as z/VM. Also, these systems must be physically and logically protected in the same way as is z/VM.
- z/VM administrators must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular:
  - All network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted.
  - Access control on security-relevant files (such as audit trails and authentication databases) must always be set up correctly.
  - Users who are authorized to access parts of the data managed by z/VM must be trained to exercise control over their own data.
- z/VM administrators must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed, installed and configured in a secure manner supporting the security mechanisms provided by z/VM.
- z/VM administrators must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.
- z/VM administrators must ensure that those parts of z/VM critical to enforcement of its security policy are protected from any physical attack that might compromise IT security objectives (for example, DASD and printers).
- z/VM administrators must ensure that procedures and/or mechanisms are provided to assure that after system failure or other discontinuity, recovery is achieved without a compromise of security.

© Copyright IBM Corp. 2005, 2024

Appendix C. Requirements for the General User

General User — Common Criteria

There are several facts that are especially useful to a Common Criteria general user, and several requirements that are important to fulfill. These are listed in the following sections.

Never Leave Your Console Terminal Unattended

Do not leave a terminal at which you are logged on unattended. To do otherwise puts your data and processes at risk. If you must leave your terminal alone, then either log off or disconnect from the system.

Do Not Add Programs to the System

The section listing the components of a z/VM software configuration fully describes the software allowed in the system. No other programs are allowed. Application programs, tools, utilities, and the like, can be added to the system, but only if, in the judgement of your system administration, they do not violate security criteria.

Carefully Protect Removable Objects

Removable objects are portable containers of data, like printed documents. The data they contain must be as secure on the removable object as it was in the system itself.

Never leave a removable object in a situation in which the data it contains becomes accessible to unauthorized parties. Consult your system administrator for details.

Periodically Change Your LOGON Password and Other Credentials

Every user of a compliant system is obliged to periodically change his or her LOGON password or password phrase. Use the RACF PASSWORD or PHRASE command or the appropriate RACF dialog, as described in the *z/VM: RACF Security Server General User's Guide*.

Your administrator determines how often these passwords must be changed. In fact, RACF will notify you when you log on that your password is due to expire. If you allow it to expire, RACF prompts you for a new password (validated by your old password).

In the case of multi-factor authentication, separate rules may apply based upon the policy or policies configured for your z/VM userid. This may involve updating certificates or updating authenticator credentials as appropriate. If using ldap-bind as a means of centralizing password use, password policies applicable to RACF may still apply to passwords stored in alternate locations.

A derived credential provided by IBM Z MFA will have a certain number of uses or time-valid and will automatically expire as appropriate.

Protect Your Credentials

Your password is integral to enforcing the identification and authentication criteria. Therefore, take extra care to prevent disclosure of your password.

Your Work May Be Audited

Security-relevant events in a Common Criteria conformant system include CP commands, DIAGNOSE functions, and communication among virtual machines. All CP events, including security-relevant events, are auditable. If your task is being audited by the system, you will not be able to tell, but be aware of the possibility.

© Copyright IBM Corp. 2005, 2024

Of course, this isn't always bad. If another user manages to tamper with your virtual machine or with your files, then an audit log of the event would help to identify the culprit.

Temporary Disks that You Receive Are Always Cleared

Whenever you define a new temporary disk (T-disk), the system clears it before it assigns it to you. That means that any residual (left-over) data that belonged to someone else is erased before you get a chance to see it.

However, that does not mean that the new T-disk is in the proper format. Each user who defines a new T-disk must format the disk before it is used.

DIAL, UNDIAL and Pre-LOGON MESSAGE Command Are Not Available

In a Common Criteria conformant system, the DIAL and UNDIAL commands are disabled. The MESSAGE command is permitted, but only after the LOGON procedure has identified and authenticated the user. Figure 7 on page 58 illustrates the LOGON prompt of a Common Criteria conformant system. The only commands that it accepts are LOGON and LOGOFF.

```
Enter one of the following commands:

   LOGON  userid (Example:  LOGON VMUSER1)
   LOGOFF
```

Figure 7. An example of the logon prompt

If you attempt to enter one of the disabled commands before you log on, you will receive the following message:

```
HCP015E Command not valid before LOGON:  command
```

where *command* is the disabled command name.

The DIAL and UNDIAL commands are always disabled in a Common Criteria conformant system. For example, if you attempt to use the DIAL command after you have logged on, you will receive the following message:

```
HCP001E Unknown CP Command:  DIAL
```

Access a second-level system by using a direct network connection or a local terminal that is attached to the guest.

Directory Changes Must be Synchronized in an SSI Cluster

A z/VM Single System Image (SSI) cluster uses a single source directory to define virtual machines on the system. Note, however, that separate object directories are built on each member node of the cluster. As a result, care must be exercised when making changes to virtual machines on the system, so that a new object directory is compiled on each member of the cluster at the same time. This can be accomplished either manually or through a directory manager program which meets security requirements. (See “Do Not Add Programs to the System” on page 57.

Failure to maintain consistency in object directories may result in integrity issues related to virtual machine behavior and discrepancies in security policy management related to the RACF configuration.

General User — CC-Secure with LSM

LSM_Begin

In addition to the Common Criteria requirements in “General User — Common Criteria” on page 57, the following apply in systems using LSM.

RACF Controls Access to Minidisks

Any attempt by any virtual machine to LINK to any minidisk, even its own, is subject to MAC testing by RACF. The same is true for all MDISK directory statements.

If access to a minidisk is requested, and if RACF denies the request, then the LINK or MDISK request fails. If an MDISK request fails, and the user is requesting MR or WR access, the user receives read-only access, but only if so authorized.

MAC checking of the MDISK directory statement ensures the security and integrity of work performed by those users authorized to use more than one SECLABEL. Whenever such users log on, MAC ensures that they receive access only to those of their minidisks whose SECLABELs are dominated by that of their current session. That is to say, no user can access even one of their own minidisks unless the SECLABEL of their current session is sufficiently dominant. That means that the only way such a user could get READ access to all of their own minidisks is to log on under a SECLABEL that dominates all of their minidisks. See “The LOGON Command” on page 44 for information on logging on under a different SECLABEL.

MAC Affects the Way You Manage Your Minidisks and Files

Some users are startled when MAC restricts, or prevents, them from performing a task they are accustomed to performing unhindered. The fact is that “The Rules of MAC” on page 11 can have implications for even the most ordinary tasks. For example, tasks involving minidisks and the files they contain. Whenever you link to a disk (whether during logon, by issuing the LINK command, or by using DIAGNOSE X'88'), MAC checks to see that the SECLABEL governing your session authorizes you to access the minidisk the way you want to access it. So, if you want READ-ONLY access, your SECLABEL must dominate that of the minidisk. And, if you want READ/WRITE access, your SECLABEL must exactly equal that of the minidisk.

Note: Users can only gain the sort of access to a disk that is appropriate to the SECLABEL under which they are logged on. Thus, it is conceivable that you might log on under a SECLABEL that gives you READ/WRITE access to none of your disks. If this proves inconvenient, you and your administrator must arrange suitable SECLABELs to give you the sort of access you need.

MAC Affects the Way You Send and Receive Data

“The Rules of MAC” on page 11 describes the rules which govern the way users share data with one another. Some examples include the SPOOL, TELL, MSG, NOTE, and SENDFILE commands.

Suppose, for instance, that you receive a message from another user in the system whose SECLABEL yours dominates. The message appears on your screen, as usual, but if you choose to respond to the message, you must alter your SECLABEL. This is because your reply wears a SECLABEL that dominates that of the other user, who, therefore, will not be able to see your reply. The only way to alter your SECLABEL is to log off and log on again under another SECLABEL, using the LOGON SECLABEL command. See “The LOGON Command” on page 44 for information on logging on under a different SECLABEL.

Suppose you receive a note, or file, from another user whose SECLABEL dominates yours. The RDRLIST command withholds much of the information about the file, because of the disparity in SECLABELs. What's more, you are unable to view the file because of its SECLABEL dominance. Furthermore, you cannot place it on your A-disk. The only options available are to log on under a different SECLABEL (see “The LOGON Command” on page 44), or to purge the file.

Privilege Class G Users Can Purge Any of Their Own Spool Files

A class G user can purge any spool file he owns, regardless of the SECLABEL designation of the file.

MAC May Cause Some Application Programs to Fail

For a user to run an application which resides on a minidisk, the SECLABEL of the user must dominate that of the minidisk.

Once an application is started, a program failure may result from input/output activity initiated from within the application. This activity is also governed by "The Rules of MAC" on page 11. For example, if you started an application, deviation from the following possible situations would cause the program to fail:

- If the application writes to a spool file, your SECLABEL must be dominated by the SECLABEL of the spool file
- If the application tries to link to a minidisk in read mode, your SECLABEL must dominate the SECLABEL of the minidisk
- If the application tries to link to a minidisk in write mode, your SECLABEL and the SECLABEL of the minidisk must be exactly equal.

Many other situation are possible and may cause a program failure. To ensure your applications are successful, always adhere to "The Rules of MAC" on page 11.

Additional Enhancements and Changes

The general user should be aware of the following Common Criteria conformance requirements, which are discussed in the following sections:

- "The LOGON Command" on page 44
- "The RACSEC Program (Querying a User's Current SECLABEL)" on page 43
- "The CP QUERY READER/PRINTER/PUNCH Command" on page 44
- "The CMS RDRLIST Command" on page 46.

LSM_End

Appendix D. Using HCPRWAC

HCPRWAC is the IBM-provided modification of HCPRWA that complies with the requirements of Common Criteria conformance. It contains the following relevant macros with the values shown:

```
RACSERV  USERID=RACFVM
RACSERV  USERID=RACMAINT
SYSSEC   DISKP=ALLOW,DISKU=FAIL,DISKF=FAIL,DISKW=FAIL,DISKM=ON,
         RDRP=ALLOW,RDRU=FAIL,RDRF=FAIL,RDRW=FAIL,RDRM=ON,
         NODEP=ALLOW,NODEU=FAIL,NODEF=FAIL,NODEW=FAIL,NODEM=ON,
         CMDP=ALLOW,CMDU=FAIL,CMDF=FAIL,CMDW=FAIL,CMDM=ON,
         LANP=ALLOW,LANU=FAIL,LANF=FAIL,LANW=FAIL,LANM=ON
         DEFLTP=ALLOW,DEFLTU=FAIL,
         DEFLTF=FAIL,DEFLTW=FAIL
```

HCPRWAC can be used if you are not able or chose not to apply your own local modifications to HCPRWA.

Note:

Using HCPRWAC requires that the VMMDISK, VMRDR, VMNODE, VMCMD, and VMLAN classes be active and resources defined for users to use any of these resources.

Do not attempt this procedure unless you have completed RACF installation and customization as described in the z/VM RACF Program Directory.

If you do not activate the VMMDISK class before IPLing CP with HCPRWAC installed, you will not be able to link to needed minidisks and will not be able to issue any RACF commands. This situation will require you to revert to your prior level of CP to correct the problem.

Add HCPRWAC to the Control Program

To add HCPRWAC to the Control Program, the list of RACF modules included in the CP kernel must be modified. Do the following:

1. Log on to the MAINT720 user ID.
2. Update the VMSES/E VM SYSSUF inventory file
    a. Use VMFUPDAT to update VM SYSSUF:

    ```
    vmfupdat syssuf
    ```

    b. Scroll through the panels to find Compname for RACF, as shown in Figure 8 on page 62. You need to change:

    ```
    :INCLUDE   YES
    ```

    to:

    ```
    :INCLUDE   CCC
    ```

    c. Press the PF5 key to process these changes.

```
                        *** Update SYSSUF Table Entries ***

 Update any PPF/component name or YES|NO field.  To change all occurrences
 of a PPF name in the table replace both ******** fields with PPF names.

 Compname         Prodid   Servlev  Prodlev  Description
 ---------------- -------- -------- -------- ---------------------------------
 RACF             7VMRAC20 000-0000 000-0000 RACF Feature of z
  :INSTALL   YES     :INSPPF   SERVP2P RACF
  :BUILD     NO      :BLDPPF   SERVP2P RACF
  :INCLUDE   CCC     :P2PPPF   SERVP2P RACFP2P
 REXX             7VMREX20 000-0000 000-0000 REXX for z/VM 7.2
  :INSTALL   YES     :INSPPF   SERVP2P REXX
  :BUILD     YES      :BLDPPF   SERVP2P REXX
  :INCLUDE   YES     :P2PPPF   SERVP2P REXXP2P
 RSCS             7VMRSC20 000-0000 000-0000 Install/Service R
  :INSTALL   YES     :INSPPF   SERVP2P RSCS
  :BUILD     YES     :BLDPPF   SERVP2P RSCS
  :INCLUDE   YES     :P2PPPF   SERVP2P RSCSP2P

 Change PPF name ******** to ********
                                                             Page 4 of 6

PF1=HELP  PF3/PF12=Quit  PF5=Process  PF6=VMFSUFTB  PF7=Backward  PF8=Forward
```

Figure 8. "Update SYSSUF Table Entries" Screen

3. Set up to force a build of the Control Program:

```
vmfsetup servp2p racf (link
vmfrepl rpiblcpn exec servp2p racf (nocopy $select
vmfsetup detach
```

4. Build RACF to incorporate HCPRWAC into the Control Program:

```
xautolog vmservp
service racf build
```

where `vmservp` is the common service filepool.

The new CP kernel, with the RACF CP parts, is placed on the secondary parm disk (default disk address of MAINT720 CF2).

For your information, a copy of the previous (or currently running) CPLOAD MODULE is still on the primary (MAINT CF1) and tertiary (MAINT CF3) parm disks as CPLOAD MODULE. It is also saved on the secondary parm disk (MAINT720 CF2) as CPLOLD MODULE.

Appendix E. Testing the Modified Control Program and Placing it into Production

Testing the Modified Control Program

Note:

In an SSI cluster, you need to perform testing of the new CP and RACF release from only one member of that cluster.

At this time, the new CP kernel is on the secondary (MAINT720 CF2) parm disk. In this step you will IPL your system with the NOAUTOLOG option. After the system IPL, XAUTOLOG the RACMAINT user ID to initialize RACF.

1. Make sure you are logged onto MAINT720 user ID to shutdown the system:

   ```
   shutdown
   ```

2. IPL the system using the MAINT720 CF2 parm disk, as this is where the new CP kernel was placed in previous step.

   To IPL from the MAINT720 CF2 parm disk you need to use the LOADPARM parameter on the IPL command; which will display the Stand-Alone Program Loader panel.

   You will need to know your console address. You can get this by doing a QUERY CONSOLE.

   Note: The following instruction can be used if you are IPLing second level. If you are IPLing first level, see the appropriate processor operator's guide for the system console for instructions.

   ```
   ipl resvoladdr clear loadparm cons
   ```

   where:

   resvoladdr
   is the address of the real DASD device containing your residence volume. (The default label is M01RES.)

   cons
   is the address of your console.

3. Change the **DEVICE NUMBER:** field to *relvoladdr*, add the IPL parameters, and press the **PF10 key** to LOAD on the Stand Alone Program Loader screen. The following is an example of this screen with the **DEVICE NUMBER:** field filled in with *relvoladdr*.

© Copyright IBM Corp. 2005, 2024

```
STAND ALONE PROGRAM LOADER: z/VM VERSION 7 RELEASE 2.0

DEVICE NUMBER:  relvoladdr     MINIDISK OFFSET:    1         EXTENT:  1

MODULE NAME:     CPLOAD     LOAD ORIGIN:       1000

--------------------------------IPL PARAMETERS--------------------------
CONS=cons fn=SYSTEM ft=CONFIG pdnum=1 pdvol=comaddr


-----------------------------------COMMENTS-----------------------------




------------------------------------------------------------------------



9= FILELIST  10= LOAD  11= TOGGLE EXTENT/OFFSET
```

Figure 9. Stand Alone Program Loader Screen

where:

relvoladdr
: is the address of the real DASD containing your release volume (default label is 720RL1, and it contains the MAINT720 CF2 parm disk).

comaddr
: is the address of the real DASD device containing your common volume (default label is VMCOM1).

4. IPL with **NOAUTOLOG**.

   When you see the following on the console:

   ```
   hh:mm:ss  Start ((Warm|Force|COLD|CLEAN) (DRain) (DIsable)  (NODIRec
   hh:mm:ss        (NOAUTOlog)) or (SHUTDOWN)
   ```

   Reply with the following, along with any other parameters you need:

   ```
   noautolog
   ```

   Answer any other replies the way you would for any other IPL of your VM system.
5. Once the system is IPLed, you need to type in the following from the system operator's console.

   ```
   xautolog racmaint
   ```
6. You can then disconnect from the operator and continue with the next task.

Placing the New CP into Production

Once you are satisfied with your testing of the RACF code using the RACMAINT user ID, place the new CP kernel on the CP production and parm disks.

When enabling the RACF Security Server for z/VM in an SSI cluster, you must perform these steps on every member of the SSI where this new release of CP and RACF are to be copied into production (note that `xautolog vmservp` is issued only on one member):

1. Log on to the MAINT720 user ID
2. Place the new CP kernel into production:

   ```
   xautolog vmservp
   xautolog vmservs
   put2prod racf
   put2prod cp
   ```
3. Log off the MAINT720 user ID

4. Initialize RACF from the system operator's console:

```
force racmaint
xautolog racfvm
```

5. At this time your system is still IPLed off of the secondary parm disk (MAINT720 CF2). The next time you IPL, you will IPL from the primary parm (MAINT CF1) disk, which is the default for IPL. If you wish, you can shutdown and IPL your z/VM system at this time.

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

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

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

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

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

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

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

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

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

© Copyright IBM Corp. 2005, 2024

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

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

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 may contain 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 may contain 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.

Programming Interface Information

This book documents information NOT intended to be used as Programming Interfaces of z/VM.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on IBM Copyright and trademark information (https://www.ibm.com/legal/copytrade).

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

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

Terms and Conditions for Product Documentation

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

Applicability

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

Personal Use

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

Commercial Use

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

Rights

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

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

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

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

IBM Online Privacy Statement

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

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

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

For more information about the use of various technologies, including cookies, for these purposes, see:

- The section entitled **IBM Websites** at IBM Privacy Statement (https://www.ibm.com/privacy)
- Cookies and Similar Technologies (https://www.ibm.com/privacy#Cookies_and_Similar_Technologies)

Bibliography

This topic lists the publications in the z/VM library. For abstracts of the z/VM publications, see *z/VM: General Information*.

Where to Get z/VM Information

The current z/VM product documentation is available in IBM Documentation - z/VM (https://www.ibm.com/docs/en/zvm).

z/VM Base Library

Overview

- *z/VM: License Information*, GI13-4377
- *z/VM: General Information*, GC24-6286

Installation, Migration, and Service

- *z/VM: Installation Guide*, GC24-6292
- *z/VM: Migration Guide*, GC24-6294
- *z/VM: Service Guide*, GC24-6325
- *z/VM: VMSES/E Introduction and Reference*, GC24-6336

Planning and Administration

- *z/VM: CMS File Pool Planning, Administration, and Operation*, SC24-6261
- *z/VM: CMS Planning and Administration*, SC24-6264
- *z/VM: Connectivity*, SC24-6267
- *z/VM: CP Planning and Administration*, SC24-6271
- *z/VM: Getting Started with Linux on IBM Z*, SC24-6287
- *z/VM: Group Control System*, SC24-6289
- *z/VM: I/O Configuration*, SC24-6291
- *z/VM: Running Guest Operating Systems*, SC24-6321
- *z/VM: Saved Segments Planning and Administration*, SC24-6322
- *z/VM: Secure Configuration Guide*, SC24-6323

Customization and Tuning

- *z/VM: CP Exit Customization*, SC24-6269
- *z/VM: Performance*, SC24-6301

Operation and Use

- *z/VM: CMS Commands and Utilities Reference*, SC24-6260
- *z/VM: CMS Primer*, SC24-6265
- *z/VM: CMS User's Guide*, SC24-6266
- *z/VM: CP Commands and Utilities Reference*, SC24-6268

© Copyright IBM Corp. 2005, 2024

- *z/VM: System Operation*, SC24-6326
- *z/VM: Virtual Machine Operation*, SC24-6334
- *z/VM: XEDIT Commands and Macros Reference*, SC24-6337
- *z/VM: XEDIT User's Guide*, SC24-6338

Application Programming

- *z/VM: CMS Application Development Guide*, SC24-6256
- *z/VM: CMS Application Development Guide for Assembler*, SC24-6257
- *z/VM: CMS Application Multitasking*, SC24-6258
- *z/VM: CMS Callable Services Reference*, SC24-6259
- *z/VM: CMS Macros and Functions Reference*, SC24-6262
- *z/VM: CMS Pipelines User's Guide and Reference*, SC24-6252
- *z/VM: CP Programming Services*, SC24-6272
- *z/VM: CPI Communications User's Guide*, SC24-6273
- *z/VM: ESA/XC Principles of Operation*, SC24-6285
- *z/VM: Language Environment User's Guide*, SC24-6293
- *z/VM: OpenExtensions Advanced Application Programming Tools*, SC24-6295
- *z/VM: OpenExtensions Callable Services Reference*, SC24-6296
- *z/VM: OpenExtensions Commands Reference*, SC24-6297
- *z/VM: OpenExtensions POSIX Conformance Document*, GC24-6298
- *z/VM: OpenExtensions User's Guide*, SC24-6299
- *z/VM: Program Management Binder for CMS*, SC24-6304
- *z/VM: Reusable Server Kernel Programmer's Guide and Reference*, SC24-6313
- *z/VM: REXX/VM Reference*, SC24-6314
- *z/VM: REXX/VM User's Guide*, SC24-6315
- *z/VM: Systems Management Application Programming*, SC24-6327
- *z/VM: z/Architecture Extended Configuration (z/XC) Principles of Operation*, SC27-4940

Diagnosis

- *z/VM: CMS and REXX/VM Messages and Codes*, GC24-6255
- *z/VM: CP Messages and Codes*, GC24-6270
- *z/VM: Diagnosis Guide*, GC24-6280
- *z/VM: Dump Viewing Facility*, GC24-6284
- *z/VM: Other Components Messages and Codes*, GC24-6300
- *z/VM: VM Dump Tool*, GC24-6335

z/VM Facilities and Features

Data Facility Storage Management Subsystem for z/VM

- *z/VM: DFSMS/VM Customization*, SC24-6274
- *z/VM: DFSMS/VM Diagnosis Guide*, GC24-6275
- *z/VM: DFSMS/VM Messages and Codes*, GC24-6276
- *z/VM: DFSMS/VM Planning Guide*, SC24-6277

- *z/VM: DFSMS/VM Removable Media Services*, SC24-6278
- *z/VM: DFSMS/VM Storage Administration*, SC24-6279

Directory Maintenance Facility for z/VM

- *z/VM: Directory Maintenance Facility Commands Reference*, SC24-6281
- *z/VM: Directory Maintenance Facility Messages*, GC24-6282
- *z/VM: Directory Maintenance Facility Tailoring and Administration Guide*, SC24-6283

Open Systems Adapter

- Open Systems Adapter/Support Facility on the Hardware Management Console (https://www.ibm.com/docs/en/SSLTBW_2.3.0/pdf/SC14-7580-02.pdf), SC14-7580
- Open Systems Adapter-Express ICC 3215 Support (https://www.ibm.com/docs/en/zos/2.3.0?topic=osa-icc-3215-support), SA23-2247
- Open Systems Adapter Integrated Console Controller User's Guide (https://www.ibm.com/docs/en/SSLTBW_2.3.0/pdf/SC27-9003-02.pdf), SC27-9003
- Open Systems Adapter-Express Customer's Guide and Reference (https://www.ibm.com/docs/en/SSLTBW_2.3.0/pdf/ioa2z1f0.pdf), SA22-7935

Performance Toolkit for z/VM

- *z/VM: Performance Toolkit Guide*, SC24-6302
- *z/VM: Performance Toolkit Reference*, SC24-6303

The following publications contain sections that provide information about z/VM Performance Data Pump, which is licensed with Performance Toolkit for z/VM.

- *z/VM: Performance*, SC24-6301. See z/VM Performance Data Pump.
- *z/VM: Other Components Messages and Codes*, GC24-6300. See Data Pump Messages.

RACF Security Server for z/VM

- *z/VM: RACF Security Server Auditor's Guide*, SC24-6305
- *z/VM: RACF Security Server Command Language Reference*, SC24-6306
- *z/VM: RACF Security Server Diagnosis Guide*, GC24-6307
- *z/VM: RACF Security Server General User's Guide*, SC24-6308
- *z/VM: RACF Security Server Macros and Interfaces*, SC24-6309
- *z/VM: RACF Security Server Messages and Codes*, GC24-6310
- *z/VM: RACF Security Server Security Administrator's Guide*, SC24-6311
- *z/VM: RACF Security Server System Programmer's Guide*, SC24-6312
- *z/VM: Security Server RACROUTE Macro Reference*, SC24-6324

Remote Spooling Communications Subsystem Networking for z/VM

- *z/VM: RSCS Networking Diagnosis*, GC24-6316
- *z/VM: RSCS Networking Exit Customization*, SC24-6317
- *z/VM: RSCS Networking Messages and Codes*, GC24-6318
- *z/VM: RSCS Networking Operation and Use*, SC24-6319
- *z/VM: RSCS Networking Planning and Configuration*, SC24-6320

TCP/IP for z/VM

- *z/VM: TCP/IP Diagnosis Guide*, GC24-6328
- *z/VM: TCP/IP LDAP Administration Guide*, SC24-6329
- *z/VM: TCP/IP Messages and Codes*, GC24-6330
- *z/VM: TCP/IP Planning and Customization*, SC24-6331
- *z/VM: TCP/IP Programmer's Reference*, SC24-6332
- *z/VM: TCP/IP User's Guide*, SC24-6333

Prerequisite Products

Device Support Facilities

- Device Support Facilities (ICKDSF): User's Guide and Reference (https://www.ibm.com/docs/en/SSLTBW_2.5.0/pdf/ickug00_v2r5.pdf), GC35-0033

Environmental Record Editing and Printing Program

- Environmental Record Editing and Printing Program (EREP): Reference (https://www.ibm.com/docs/en/SSLTBW_2.5.0/pdf/ifc2000_v2r5.pdf), GC35-0152
- Environmental Record Editing and Printing Program (EREP): User's Guide (https://www.ibm.com/docs/en/SSLTBW_2.5.0/pdf/ifc1000_v2r5.pdf), GC35-0151

Related Products

XL C++ for z/VM

- *XL C/C++ for z/VM: Runtime Library Reference*, SC09-7624
- *XL C/C++ for z/VM: User's Guide*, SC09-7625

z/OS

IBM Documentation - z/OS (https://www.ibm.com/docs/en/zos)

Index

A

activating classes 21
APPC connect 52
APPC password validation 52
ATTACH command 49
audit records 19, 29, 32, 33
audit records, transfer of 36
audit reports 36
audit, read-only 36
auditability of security-relevant events 2
auditing options 20
AUTOLOG command 49

C

CHANGE command 45, 49
CLOSE command 49
commands
  ATTACH 49
  AUTOLOG 49
  CHANGE 45, 49
  CLOSE 49
  COUPLE 49
  DEFSEG 49
  DEFSYS 49
  DIAL 49, 58
  FOR 49
  GIVE 49
  IPL 50
  LINK 50
  LOGOFF 50
  LOGON 44, 50
  MESSAGE 50, 58
  MSGNOH 50
  QUERY 50
  QUERY rdev 50
  QUERY READER/PRINTER/PUNCH 44
  QUERY TAG 50
  QUERY TRFILES 50
  QUERY.READER/PRINTERPUNCH 50
  RDRLIST 46
  RESET 50
  RVARY
    SETEVENT 37
  SEND 50
  SET LOGMSG 50
  SET OBSERVER 34, 50
  SET PASSWORD 50
  SET PRIVCLAS 50
  SET SECUSER 34, 50
  SET SMSG 50
  SETRACF 36
  SETROPTS 20, 37
  SPOOL 50
  START 39, 50
  STORE 50
commands *(continued)*
  TAG 34
  TAG DEVICE 50
  TAG FILE 50
  TAG QUERY 51
  TRANSFER 51
  TRSAVE 51
  TRSOURCE 51
  UNDIAL 51, 58
  VMDUMP 51
  VMRELOCATE 51
  WNG 51
  XAUTOLOG 51
common criteria 1
Common Criteria 39
Common Criteria certification xv
COUPLE command 49
CP command issued from directory 52
CP commands, security-relevant 49
CP DIAL command 20
CP START command 39
CP system directory 27

D

DAC 2
DEFSEG command 49
DEFSYS command 49
DIAGNOSE code X'BC' 45
DIAGNOSE code X'D4' 46
DIAGNOSE X'04' 51
DIAGNOSE X'08' 51
DIAGNOSE X'14' 51
DIAGNOSE X'23C' 52
DIAGNOSE X'34' 51
DIAGNOSE X'4C' 51
DIAGNOSE X'64' 51
DIAGNOSE X'68' 51
DIAGNOSE X'74' 52
DIAGNOSE X'7C' 52
DIAGNOSE X'84' 52
DIAGNOSE X'88' 52
DIAGNOSE X'90' 52
DIAGNOSE X'94' 52
DIAGNOSE X'98' 52
DIAGNOSE X'A0' 52
DIAGNOSE X'B8' 52
DIAGNOSE X'BC' 52
DIAGNOSE X'CC' 52
DIAGNOSE X'D4' 52
DIAGNOSE X'E0' 52
DIAGNOSE X'E4' 52
DIAGNOSE X'FC' 52
DIAL command 49, 58
directory changes
  SSI cluster 58
discretionary access control 2

DTCPARMS operands, required 17
dumps 29

E

entropy, validation of 32
evaluation assurance level 1

F

find restricted segment 52
FOR command 49

G

GAC 35
general user 57
GIVE command 49
global access checking 30, 35

H

hardware virtualization 3
human-readable labels 24

I

identification and authentication 2
IMG files 31
IPL command 50
IUCV connect 52

L

labeled security mode 3
labeled security mode (LSM) 9
LINK 59
LINK command 50
LINK requests 28
load restricted segment 52
logging options 20
LOGOFF command 50
LOGON command 44, 50
LOGON password 57
LSM 3, 9

M

MAC 4, 11
manadatory access control 11
mandatory access control (MAC) 4
MDISK 52, 59
MDISK requests 28
MESSAGE command 20, 50, 58
messages 34
MSG command 20
MSGNOH command 50
multi-factor authentication 37

N

named objects 5
NSS 31
number generation, random 32

O

object reuse 2
objects 5
operands, required DTCPARMS 17
operating system functionality virtualization 3
OSPP-VIRT 3

P

password 57
password encryption policy 20
password policy 20
password suppression 16
performance considerations 35
print of spool file 52
printing system 39
privilege 7
programming interface information 68
protection profile 1
public objects 6

Q

QUERY command 50
QUERY rdev command 50
QUERY READER/PRINTER/PUNCH command 44
QUERY TAG command 50
QUERY TRFILES command 50
QUERY.READER/PRINTERPUNCH command 50
querying a user's current SECLABEL 43

R

RACF
  customizing 18, 20
  initialization options 18
  installing 18
  privilege 8, 36
  profiles 35
  resource profiles 21
  SECLABEL class 24
  service machines 34
  SETRACF command 36
  SETROPTS command 20
  SEVER option 19
RACSEC program 43
random number generation 32
RDRLIST command 46
read-only audit 36
READ-ONLY rule 12
READ/WRITE rule 12
required DTCPARMS operands 17
reserved security labels 12
RESET command 50
resource classes 21
resource profiles 21
restricted segment 52

S

saved segments 31
SECLABEL
    defining 21
    overview 9
SECLABEL class 24
SECTABLE application 42
secure system initialization 15
security labeling 4, 9
security target 1
security-relevant CP commands 49
SEND command 50
server virtualization functionality 3
SET LOGMSG command 50
SET OBSERVER command 50
SET PASSWORD command 50
SET PRIVCLAS command 50
SET SECUSER command 50
SET SMSG command 50
SETRACF command 36
SETROPTS command 20
SEVER option 19
shared RACF database 37
single system image (SSI) 37
sniffer state change 53
SPOOL command 50
spool file create 52
spool file delete 53
spool file open 53
spool file print 52
START command 39, 50
storage objects 6
STORE command 50
subjects 4
system data file create 53
system data file delete 53
system data file open 53
system directory 27
system dumps 29
system operator 28

T

TAG command 34
TAG DEVICE command 50
TAG FILE command 50
TAG QUERY command 51
target of evaluation 1
TCP/IP
    customizing 17
    initialization options 17
    installing 17
temporary disks 16
TLS connections 32
TOE 1
TRANSFER command 51
transfer of audit records 36
TRSAVE command 51
TRSOURCE command 51
trusted servers 22

U

UNDIAL command 51, 58

V

validation of entropy 32
virtual network sniffer state change 53
VMDUMP command 51
VMGROUP option 31
VMRELOCATE command 51

W

WNG command 51
WRITE-ONLY rule 12

X

XAUTOLOG command 51

Z

z/VM Management Network 28

Product Number: 5741-A09

Printed in USA

SC24-6323-05