IBM Security zSecure Manager for RACF z/VM

Efficient security administration and audit in virtual environments

Highlights

- Automate complex, time-consuming IBM® z/VM® security management tasks with simple, one-step actions that can be performed without detailed knowledge of IBM Resource Access Control Facility (RACF®) command syntax
- Create efficient, comprehensive audit trails and compliance reports to measure and verify the effectiveness of the z/VM security and compliance policies without substantial manual effort
- Help ease the burden of database and system consolidations

Security is a cornerstone of any organization's controls environment—it is essential to effective protection against IT threats. Security breaches can cause everything from financial losses to damaging publicity as a result of unauthorized access to confidential information and theft of intellectual property. Because of these risks, the IT staff is challenged to provide detailed audit and controls documentation while facing increasing demands on their time due to mergers, reorganizations and other changes.

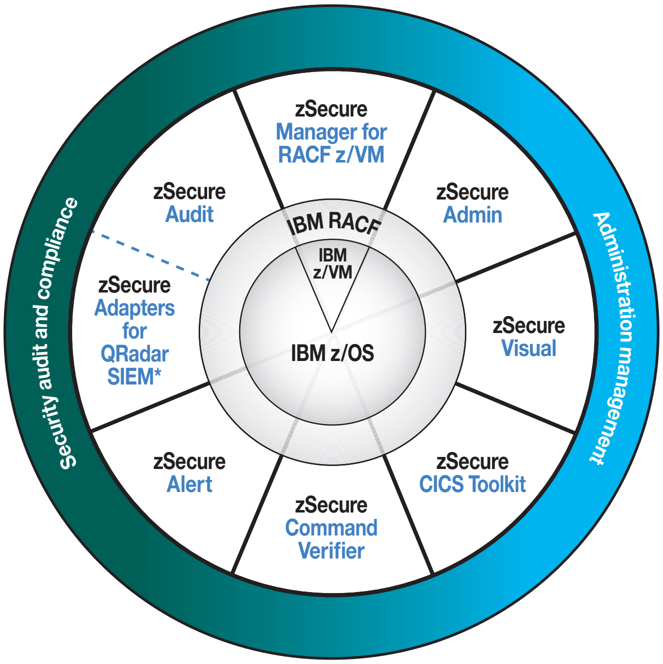
As the standard security system for mainframes running z/VM, RACF plays a vital role in helping to protect mainframes from unauthorized entry and misuse by authorized users. But the ultimate strength of your mainframe security system lies in the people who manage it, which makes it critical that you furnish administrators with the tools needed to perform their work as efficiently as possible. However, helping ensure that the IT staff is sufficiently skilled and leveraging the power inherent in RACF can be challenging.

Many organizations utilize their mainframe to help ease the burden of database and system consolidations. They can exploit the mainframe as their enterprise security hub using a variety of options, including logical partitions (LPARs), z/VM, Linux for IBM z Systems™ and Integrated Facility for Linux (IFL). Organizations can establish the mainframe as their secure, private cloud computing platform running virtualized workloads.

IBM Security zSecure™ Manager for RACF z/VM provides administrators with tools to help unleash the potential of their mainframe system—enabling efficient and effective RACF administration using fewer resources. By automating many recurring system administration functions, zSecure Manager for RACF z/VM can help you maximize IT resources, reduce errors, minimize complexity, improve quality of service, demonstrate compliance and reduce costs.

In addition to effectively managing administration, security audits are another way organizations avoid potential security breaches. However, gathering the necessary information can be an overwhelming, stressful and time-consuming process. One way to help avoid last-minute audit scrambles is to develop a repeatable, automated process for auditing and reporting. The zSecure Manager for RACF z/VM solution provides auditing capabilities designed to help RACF users efficiently measure and verify the effectiveness of their z/VM security and compliance policies. Using automatically generated reports in a standard format, you can quickly locate problems with attributes around a particular resource. As a result, you can reduce errors and improve overall quality of services.

IBM Security zSecure suite



* Product offers a subset of the capabilities provided by zSecure Audit

The IBM Security zSecure suite consists of a collection of solutions—including IBM Security zSecure Manager for RACF z/VM—to help ensure security and compliance on z System mainframes.

zSecure Manager for RACF z/VM is part of the IBM Security zSecure suite, which helps improve the efficiency and maintainability of the mainframe security environment. Applicable features of IBM Security zSecure Admin and IBM Security zSecure Audit components for IBM z/OS® form the foundation for the functionality of zSecure Manager for RACF z/VM.

Automate routine tasks to help simplify administration

Easy to install and deploy, zSecure Manager for RACF z/VM offers robust, nonintrusive security capabilities designed to help simplify the process of managing z/VM security. The result enables you to simplify complex tasks using one-step actions that can be performed without extensive RACF knowledge and only minimal training. Queries can be executed in seconds, and mass changes can be implemented with little administration. zSecure Manager for RACF z/VM enables you to automate recurring, time-consuming security tasks, such as:

- Adding or deleting user IDs and groups
- Defining and granting access to users and user groups
- Setting and resetting user IDs and passwords
- Displaying all occurrences or a cross-reference of a user ID or a user group
- Running daily or monthly reports

Identify and analyze problems to help minimize threats

After auditing and analyzing the z/VM operating system and RACF database, zSecure Manager for RACF z/VM prioritizes and highlights security concerns. It provides displays to view vital z/VM information and identifies problems that might require further investigation. Problems are ranked by audit priority with a number indicating the relative impact of a problem.

zSecure Manager for RACF z/VM can help you quickly identify RACF problems on the z/VM operating system, such as missing or inconsistent definitions, enabling you to fix or prevent mistakes before they become a threat to security and compliance. You can also monitor privileged users to help ensure that old accounts are properly deleted and that products have been integrated appropriately—thereby helping avoid vulnerabilities that can be exploited by other users.

In addition, you can request information about individual definitions in RACF or unload all RACF profiles to an external database such as IBM DB2® for offline analysis and reporting.

zSecure Manager for RACF z/VM includes support for auditing events from Linux on IBM z Systems. Auditing these event records helps detect Linux security threats and creates compliance reports for Linux systems consolidated on IBM zEnterprise® systems or on previous releases of z Systems This is accomplished by auditing System Management Facility (SMF) record type 83-4 on z/VM, which can contain events from Linux on z Systems.

zSecure Manager for RACF z/VM can also assess and report changes in basic security settings, including the following:

- Support for basic RACF settings contained in the RACF/VM module HCPRWA
- Protection of virtual and real devices
- Active settings for the protection and auditing of Control Program (CP) commands and for diagnosing application program interface (API) calls

Merge databases quickly and efficiently

In today's ever-changing business world—where mergers and acquisitions are a frequent fact of life—flexibility is essential, especially where database management is concerned. zSecure Manager for RACF z/VM helps ease the burden of consolidation efforts by enabling you to:

- Efficiently merge security rules from different databases
- Copy or move users, groups, resources, applications or whole databases between systems
- Rename IDs within the same database

In addition, when merging profiles from different databases, zSecure Manager for RACF z/VM performs extensive consistency checks and reports potential conflicts before generating commands.

Customize reports to meet specific needs

You have the option of using zSecure Manager for RACF z/VM to produce reports in email format on a daily or custom schedule, only when specific events occur, or when there is a security breach. Extensive reporting capabilities also include the ability to:

- Generate reports in XML format
- Import report data into databases and reporting tools
- View data with Microsoft Internet Explorer or Microsoft Excel
- Exploit workstation scrolling capabilities
- Allow managers to view, sort and annotate audit reports
- Produce reports centrally for automatic distribution to decentralized groups
- Combine multiple reports in a single bundle for automatic distribution
- Save reports directly on the web server, thus allowing the reports to be accessible through the intranet
- Produce machine-readable reports for input into post-processing programs on z/VM or other platforms
- Include audit reports for Linux on z Systems

The CARLa Auditing and Reporting Language (CARLa) used in zSecure Manager for RACF z/VM enables you to modify the displays and reports. Reports can be run under IBM Interactive System Productivity Facility (ISPF) or in batch, using data from any RACF database, live or extracted RACF System Management Facility (SMF) data, or unloaded data—without changing the CARLa programs.

Analyze RACF profiles to get fast answers

To analyze the defined user, group, data set and resource profiles or entries, zSecure Manager for RACF z/VM reads and updates the RACF database directly from an OS-formatted disk or can use a copied or unloaded RACF database (support for the live RACF database is available only if the database is accessible from a Conversational Monitor System [CMS] minidisk). The selected records are shown in an ISPF scrollable display with detailed information available on request or in a printable report. You can search on any field in the profiles and answer questions such as “Who has access to this file?” and “Which system specials have not changed their passwords?” You can create and view these reports interactively under ISPF or run them automatically in batch and view them in a format suitable for printed reports.

You can also include information from external files in your RACF profile displays and reports to help reduce organizational costs. For example, you can match human resource information with user profiles and include that information in the reports.

Analyze SMF log files to create a comprehensive audit trail

zSecure Manager for RACF z/VM analyzes SMF information from the live SMF data or from extracted SMF data on tape or disk. By using live data, information from the active system can be viewed interactively immediately after an event has occurred.

Leverage external file support to make reports highly usable

zSecure Manager for RACF z/VM can support external files of existing data. It can filter external supplementary information from existing data sources and corporate applications (such as unit, department and personnel data) and present it alongside the technical data from z/VM and RACF in automatically generated reports.

Ease compliance reporting with a new automation interface

zSecure Manager for RACF z/VM now includes the ability to ease compliance reporting with a new interface to automate reporting about external security standards, including the newer external standards for the Defense Information Systems Agency (DISA), Security Technical Implementation Guide (STIG), Payment Card Industry Data Security Standard (PCI DSS) and IBM Outsourcing GSD331 (or iSeC), which is the primary IBM information security controls documentation for customers of IBM Strategic Outsourcing services.

Detect integrity breaches

zSecure Manager for RACF z/VM includes a powerful system integrity analysis feature that can help reveal breaches in system integrity and other irregularities. Reports identify exposures and potential threats based on intelligent analysis built into the system. These reports rank the severity of the exposure and provide a description that helps you determine the corrective action required.

zSecure Manager for RACF z/VM administration and audit functions are very similar to the IBM Security zSecure Admin and Audit functions on z/OS. Data collected by the former on z/VM can be analyzed together with z/OS data by the latter under z/OS. If users have both products, they can integrate data from both using IBM Security QRadar® SIEM.

IBM Security zSecure Manager for RACF z/VM at a glance

System requirements:
- z/VM
- RACF

Why IBM?

zSecure Manager for RACF z/VM helps deliver the same measure of extended security that is available on the z/OS platform to virtual systems on the mainframe. It offers simplified security administration, comprehensive audit reporting and other features that demonstrate compliance, minimize complexity and help reduce costs. Users can better leverage the mainframe as their enterprise security hub with enhanced protection and secure consolidation of their virtual systems.

For more information

To learn more about IBM Security zSecure Manager for RACF z/VM, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

© Copyright IBM Corporation 2015

Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
February 2015

IBM, the IBM logo, ibm.com, DB2, RACF, zEnterprise, zSecure, z/OS, z/VM, z Systems, QRadar, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

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

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Please Recycle