IBM Security zSecure Audit

Deliver comprehensive mainframe security audit reporting and compliance analysis

Highlights

- Help lower the cost of event collection from many products, and automate audit analysis for repeatable and sustainable reporting
- Identify security weaknesses to help minimize the risk of costly breaches
- Leverage tailored reporting to generate baseline verifications of security

Security is a cornerstone of any organization’s control environment, and in today’s networked economy, it is essential to have effective protection against IT threats. Security breaches can result in financial losses, unauthorized access to confidential information, theft of intellectual property, service disruption and damaging publicity.

While audits can help organizations avoid these problems, gathering the necessary information can be a stressful, time-consuming process. One way to help avoid last-minute audit scrambles is to implement a repeatable, sustainable and automated process for auditing and reporting.

IBM® Security zSecure™ Audit is a mainframe tool designed to help security personnel for IBM Resource Access Control Facility (IBM RACF®), CA-ACF2 and CA Top Secret security efficiently measure and verify the effectiveness of their mainframe security and security policies. Automatically generated reports in a standard format help to quickly locate problems with attributes around a particular resource (such as authorized programs) thus providing vulnerability analysis of your mainframe infrastructure. As a result, you can reduce errors and improve overall quality of service. zSecure Audit also helps expert users extend and enrich security by enforcing and enhancing security policies.

zSecure Audit is designed to help an enterprise:

- Gather and analyze critical information efficiently
- Support security information and event management
- Customize reports to meet specific needs
- Analyze RACF profiles and ACF2 entries to get fast answers

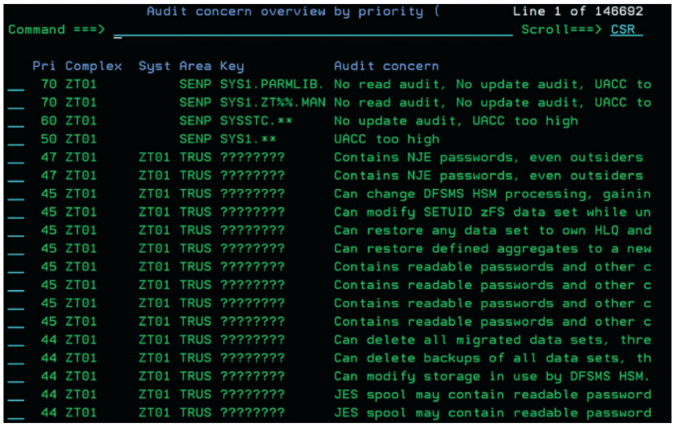
- Analyze system management facilities (SMF) log files to create a comprehensive audit trail
- Ease compliance reporting with a new automation interface
- Leverage external file support to make reports highly usable
- Detect system changes to minimize security risks
- Track and monitor baseline changed for RACF and ACF2
- Detect integrity breaches
- Support IBM Security Guardium® Vulnerability Assessment, IBM QRadar® SIEM, IBM Common Data Provider for z Systems®, IBM Multi-Factor Authentication for z/OS® (IBM MFA) and the pervasive encryption feature of IBM Z®.

Gather and analyze critical information efficiently

Unlike offerings that report on only a copy of a database, zSecure Audit allows you to access live security data on mainframes running IBM z/OS with RACF, ACF2 or Top Secret, delivering up-to-the-minute audit accuracy. It also analyzes the active z/OS system control blocks and can help you quickly identify the following:

- RACF profiles, ACF2 logon IDs and rules
- CA Top Secret SMF security records
- Questionable definitions
- RACF access lists and ACF2 rule entries
- System options
- Flawed settings
- Exceptions such as changes to the z/OS parameters, profiles and options; system and user libraries; and customized, installation-specific items
- Visibility over who can modify your trusted computing base

After auditing and analyzing the z/OS operating system, zSecure Audit prioritizes and highlights security concerns. It provides displays to view definitions, tables, exits and other vital z/OS information and identifies problems or potential problems. Problems are ranked by audit priority using a number to indicate the relative impact of a problem.



```
                 Audit concern overview by priority (         Line 1 of 146692
Command ===> _________________________________________________ Scroll===> CSR

   Pri Complex  Syst Area Key           Audit concern
__  70 ZT01          SENP SYS1.PARMLIB. No read audit, No update audit, UACC to
__  70 ZT01          SENP SYS1.ZT%%.MAN No read audit, No update audit, UACC to
__  60 ZT01          SENP SYSSTC.**     No update audit, UACC too high
__  50 ZT01          SENP SYS1.**       UACC too high
__  47 ZT01     ZT01 TRUS ????????      Contains NJE passwords, even outsiders
__  47 ZT01     ZT01 TRUS ????????      Contains NJE passwords, even outsiders
__  45 ZT01     ZT01 TRUS ????????      Can change DFSMS HSM processing, gainin
__  45 ZT01     ZT01 TRUS ????????      Can modify SETUID zFS data set while un
__  45 ZT01     ZT01 TRUS ????????      Can restore any data set to own HLQ and
__  45 ZT01     ZT01 TRUS ????????      Can restore defined aggregates to a new
__  45 ZT01     ZT01 TRUS ????????      Contains readable passwords and other c
__  45 ZT01     ZT01 TRUS ????????      Contains readable passwords and other c
__  45 ZT01     ZT01 TRUS ????????      Contains readable passwords and other c
__  45 ZT01     ZT01 TRUS ????????      Contains readable passwords and other c
__  44 ZT01     ZT01 TRUS ????????      Can delete all migrated data sets, thre
__  44 ZT01     ZT01 TRUS ????????      Can delete backups of all data sets, th
__  44 ZT01     ZT01 TRUS ????????      Can modify storage in use by DFSMS HSM.
__  44 ZT01     ZT01 TRUS ????????      JES spool may contain readable password
__  44 ZT01     ZT01 TRUS ????????      JES spool may contain readable password
```

Audit concerns from an automated status audit.

zSecure Audit can also provide extensive audit and analysis capabilities beyond the conventional z/OS components, including the ability to audit UNIX security definitions on the mainframe and automatically find problems within the security definitions in the UNIX subsystem. In addition, zSecure Audit provides audit support for security events from Linux on IBM z Systems, IBM Db2®, IBM Customer Information Control System (CICS®), IBM MQ for z/OS, IBM Information Management System (IMS™) security settings and audit security events from IBM Security Key Lifecycle Manager for z/OS, IBM WebSphere® Application Server, IBM Tivoli® OMEGAMON®, hierarchical storage management, IBM Communications Server network configuration for TCP/IP, PDS(E) member-level auditing, IBM MFA events and pervasive encryption information including z/OS Encryption Readiness Technology (zERT).

Support security information and event management

Audit events and user access logs generated by IBM security management tools can be populated within QRadar SIEM for normalization and compliance reporting. This integration harmonizes the collection infrastructure among the product lines, thereby supporting an effective, comprehensive security information and event management solution.

Integration with QRadar SIEM enhances security intelligence by providing:

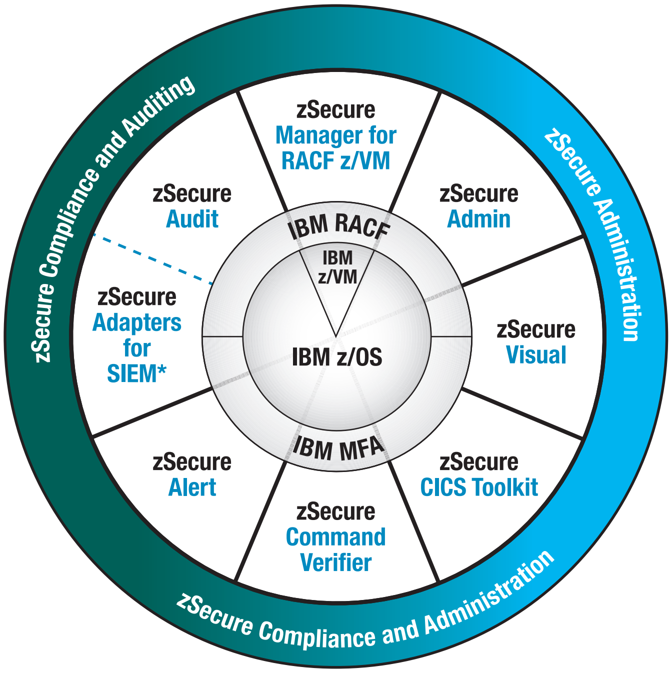
- Integrated log, threat, risk and compliance management
- Sophisticated event analytics
- Asset profiling and flow analytics
- Offense management and workflow

Customize reports to meet specific needs

At your option, zSecure Audit can email reports on a daily basis 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 using Microsoft Internet Explorer, Mozilla Firefox 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 an intranet
- Produce machine-readable reports for input into post-processing programs on z/OS or other platforms
- Build installation-specific system, RACF, ACF2, Top Secret and SMF reports

IBM Security zSecure suite



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

This diagram is a summary of products that comprise the IBM Security zSecure suite, including IBM Security zSecure Audit.

The CARLa Auditing and Reporting Language (CARLa) used in zSecure Audit enables you to modify the displays and reports using SMF and other data sources. Using the DEFINE command, you can add your own variables to zSecure Audit to map and report on installation-specific information. These variables can be used in select and output functions. This reduces the need to write reports in other programming languages.

Reports can be run under IBM Interactive System Productivity Facility (ISPF) or in batch on any RACF or ACF2 database, live or extracted SMF data sets or on unloaded data—without requiring any changes to the CARLa programs. The reports can also analyze the HTTP access and error log to see who is accessing or using data on the internal IT environment through the Internet.

zSecure Audit also allows you to send Simple Network Management Protocol (SNMP) or syslog messages to an enterprise management console for policy exceptions or violations that indicate a security breach or weakness.

Analyze RACF profiles and ACF2 entries to get fast answers

zSecure Audit uses the active or unloaded RACF database or ACF2 database to analyze the defined user and group IDs, and the dataset and resource profiles. The selected records can be output to a printable report or to an ISPF scrollable display with detailed information available on request. You can search on any field in the profiles and answer questions such as “Who has access to this data set?” and “Who are the system special users who have not changed their password?” You can generate these reports interactively from the ISPF interface or run them automatically in batch. Support for ACF2 role-based security, where access is based on users and roles rather than a UID string, can simplify user administration and improve compliance.

Analyze SMF log files to create a comprehensive audit trail

zSecure Audit analyzes SMF from live SMF data sets, from extracted SMF data on tape or disk, or from a Logstream. The SMF analysis component supports more than 50 standard z/OS SMF record types and includes specific auditing functions for RACF, ACF2, Top Secret, Db2, CICS, IMS, MQ, Tivoli OMEGAMON, UNIX, Linux on z Systems, WebSphere Application Server, IBM Security Key Lifecycle Manager for z/OS, Integrated Cryptographic Service Facility (ICSF), IBM Communications Server, IBM MFA, pervasive encryption and more. You can produce overview and detail reports about system and user activity from the SMF log files. On z/OS systems with Top Secret, the Audit/Tracking File can also be used.

By using live data sets, information from the active system can be viewed interactively immediately after an event has taken place. zSecure Audit can remember the RACF user ID for each IBM Time Sharing Option (TSO) session, batch job or started task it finds in SMF. Subsequently, SMF records from the same task are tagged with this information. This allows you to create an audit trail of a specific user ID using SMF data.

Ease compliance reporting with a new automation interface

zSecure Audit 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.

Leverage external file support to make reports highly usable

zSecure Audit can support external files of existing data. It can filter external supplementary information from existing databases and corporate applications (such as unit, department and personnel data) and present this information alongside the technical data from z/OS, RACF, ACF2 and Top Secret in automatically generated reports. For example, if a policy exception takes place, such as logging in after work hours, then information about the user (name, matching user ID, department, email address and telephone details) is gathered from the personnel database.

Detect system changes to help minimize security risks

zSecure Audit can identify changes in the individual members of partitioned data sets using digital signatures for each member of the libraries under scrutiny. zSecure Audit indicates whether a member was added, deleted or changed. For load modules, zSecure Audit also identifies program temporary fixes (PTFs) and zaps applied to modules, and then reports the differences between two or more PTFs.

zSecure Audit can identify identical members in the same or different libraries, identically named members with different contents and load module members touched by PTFs and zaps. zSecure Audit also provides a starter set that contains sample daily reports to automatically identify changes and ISPF dialogs to check your system.

The same digital fingerprint technology can be used to verify the authenticity of log files and help you demonstrate that logs were not tampered with—which is important for both security and compliance initiatives.

To help further reduce the risk of damage, you can deploy IBM Security zSecure Command Verifier, which verifies each RACF command against your security policy and prevents noncompliant commands from being run—before any damage is done.

Track and monitor baseline changes for RACF and ACF2

zSecure Audit can help you define a baseline for RACF and ACF2 security parameters such as profile and parameter settings and monitor the baseline settings against current system settings to detect changes. Detected changes can be used to update the baseline or tagged for follow-up actions such as security reviews. You can also add installation and application-specific settings to the baseline such as profiles for application data sets, the mandatory inactivity of emergency user IDs, or profiles accessible to specific users.

Help detect integrity breaches

zSecure Audit includes a powerful system integrity analysis feature that can help reveal breaches in system integrity and other irregularities. Reports identify potential exposures and threats based on built-in intelligent analysis. These reports rank the severity of the exposure and help you determine the type of corrective action required.

In addition, zSecure Audit checks for and enforces program signatures to support the PCI DSS. Using zSecure Audit in conjunction with IBM Security zSecure Admin, you can also configure the system response to allow, audit or fail requests initiated by programs without valid signatures. zSecure Audit integrates smoothly with zSecure Admin for end-to-end closed-loop monitoring and remediation. Seamless integration with zSecure Admin enables administrators to move quickly to diagnose and remediate security failures or exposures.

zSecure Audit also integrates with QRadar SIEM so that you can incorporate mainframe security information into a broader, enterprise-level audit and compliance solution. IBM Security zSecure Adapters for SIEM provides a separate subset of zSecure Audit capabilities, which also sends enriched mainframe security information to IBM QRadar Security Intelligence Platform and other security information and event management (SIEM) solutions to integrate reporting and analysis.

Support IBM Security Guardium Vulnerability Assessment

zSecure Audit can provide information about access to Db2 objects as input to Guardium Vulnerability Assessment for both Db2 internal and external (RACF or ACF2) security. This integration allows a high-performance interface for evaluating vulnerabilities and security best practices in Db2 subsystems using either internal security or external (RACF or ACF2) security through the System Authorization Facility (SAF).

Integration with Guardium Vulnerability Assessment enhances security intelligence by providing:

- Analysis of Db2 object types including access control information, system, database and direct privileges
- Reports, including warnings of situations where security best practices are not implemented
- Fast access to the complete list of all users with access to critical data stored in Db2

Why IBM?

IBM Security zSecure Audit offers one of the leading solutions to help organizations ease the burden of audit preparation and analysis and compliance reporting. zSecure Audit integrates seamlessly with the complete IBM Security zSecure suite of enterprise-wide security auditing solutions, providing an end-to-end workbench for RACF security management.

For more information

To learn more about IBM Security zSecure Audit, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/us-en/marketplace/zsecure-audit

For more information on IBM Security, please visit: **ibm.com**/security

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.

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
September 2017

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 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