Tivoli® software

IBM Tivoli zSecure Audit

Highlights

- Help lower cost of event collection and analysis
- Identify security weaknesses to help you minimize the risk of costly breaches
- Leverage tailored reporting to generate baseline verifications of security
- Track and monitor baseline and library changes
- Help mitigate RACF security risks from same interface
- Versions for RACF, CA ACF2 and CA TSS available

Security is a cornerstone of any corporation's controls environment, and in today's networked economy, it is essential to have effective protection against IT threats. Security breaches can result in everything from financial losses and unauthorized access to confidential information to theft of intellectual property 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, automated process for auditing and reporting.

IBM Tivoli® zSecure Audit is an audit tool for mainframes, designed to help IBM Resource Access Control Facility (RACF®), CA ACF2™ and CA Top Secret® Security (TSS) users efficiently measure and verify the effectiveness of their mainframe security and security policies. By viewing automatically generated reports in a standard format, you can quickly locate problems with attributes around a particular resource (such as an unprotected data set). As a result, you can reduce errors and improve overall quality of services. Designed to help RACF, ACF2 and TSS users perform tasks more efficiently, Tivoli zSecure Audit also helps expert users extend and enrich security by enforcing and enhancing security policies.

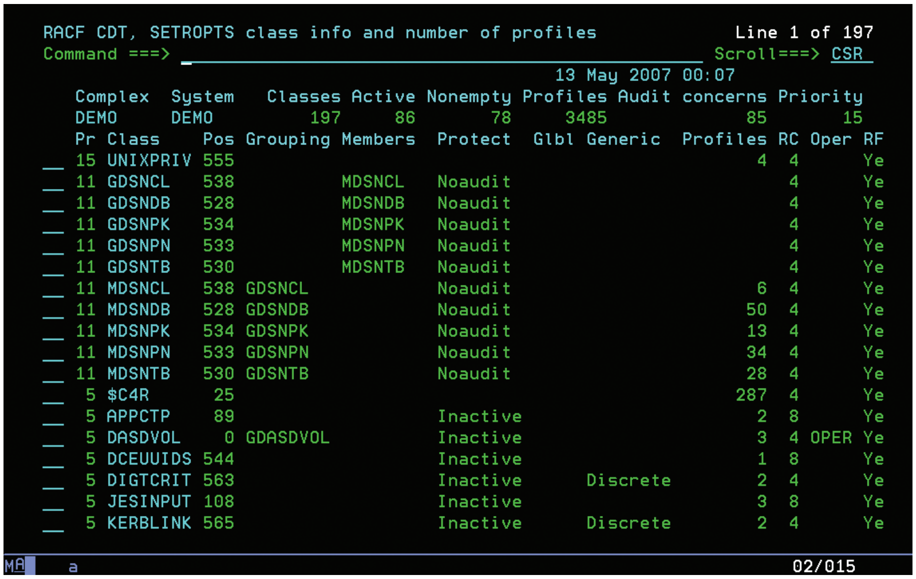
Gather and analyze critical information efficiently

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

- RACF profiles, ACF2 logon IDs/ACF2 rules, TSS Accessor IDs (ACIDs)/TSS permits
- Questionable definitions
- RACF access lists and ACF2 rule entries
- Systems options
- Flawed settings
- Exceptions, such as changes to the z/OS parameters, profiles and options, system and user libraries, and customized, installation-specific items

After auditing and analyzing the z/OS operating system, Tivoli zSecure Audit prioritizes and highlights security concerns. It provides displays to view definitions, tables, exits and other vital z/OS information and indicates where it found problems. Problems are ranked by audit priority, with a number indicating the relative impact of a problem.

Tivoli zSecure Audit can also provide audit and analysis capabilities beyond z/OS systems, including the ability to audit security definitions of UNIX® on the mainframe and automatically find problems in the security definitions in the UNIX subsystem. In addition, Tivoli zSecure Audit provides support for IBM DB2® audit events, enabling you to view activity within DB2 systems on the mainframe.



```
RACF CDT, SETROPTS class info and number of profiles             Line 1 of 197
Command ===> _________________________________________________ Scroll===> CSR
                                                13 May 2007 00:07
   Complex  System   Classes Active Nonempty Profiles Audit concerns Priority
   DEMO     DEMO          197     86       78     3485             85       15
   Pr Class    Pos Grouping Members  Protect  Glbl Generic  Profiles RC Oper RF
__ 15 UNIXPRIV 555                                                 4  4      Ye
__ 11 GDSNCL   538          MDSNCL   Noaudit                          4      Ye
__ 11 GDSNDB   528          MDSNDB   Noaudit                          4      Ye
__ 11 GDSNPK   534          MDSNPK   Noaudit                          4      Ye
__ 11 GDSNPN   533          MDSNPN   Noaudit                          4      Ye
__ 11 GDSNTB   530          MDSNTB   Noaudit                          4      Ye
__ 11 MDSNCL   538 GDSNCL            Noaudit                       6  4      Ye
__ 11 MDSNDB   528 GDSNDB            Noaudit                      50  4      Ye
__ 11 MDSNPK   534 GDSNPK            Noaudit                      13  4      Ye
__ 11 MDSNPN   533 GDSNPN            Noaudit                      34  4      Ye
__ 11 MDSNTB   530 GDSNTB            Noaudit                      28  4      Ye
__  5 $C4R      25                                               287  4      Ye
__  5 APPCTP    89                   Inactive                      2  8      Ye
__  5 DASDVOL    0 GDASDVOL          Inactive                      3  4 OPER Ye
__  5 DCEUUIDS 544                   Inactive                      1  8      Ye
__  5 DIGTCRIT 563                   Inactive      Discrete        2  4      Ye
__  5 JESINPUT 108                   Inactive                      3  8      Ye
__  5 KERBLINK 565                   Inactive      Discrete        2  4      Ye
MA     a                                                             02/015
```

This display shows the classes defined to a particular RACF system, sorted by audit priority, so you can quickly locate problems. You can then zoom in on a class of interest for a screen with the relevant details.

Customize reports to meet specific needs

At your option, Tivoli zSecure Audit can deliver e-mailed reports on a daily basis, 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/OS or other platforms.

The Consul Auditing and Reporting Language (CARLa) used in Tivoli zSecure Audit enables you to modify the displays and reports, and build installation-specific system, RACF,

ACF2, TSS and System Management Facility (SMF) reports. With the DEFINE command you can add your own variables to Tivoli zSecure Audit, to map installation-specific information and use these in select and output functions.

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 changing 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.

Tivoli zSecure Audit also allows you to send Simple Network Management Protocol (SNMP) 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

Tivoli zSecure Audit uses the active or unloaded RACF database or ACF2 database to analyze the defined user, group, data set and resource profiles/entries. The selected records are shown in an ISPF scrollable display with detail 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 data set?” and “List all system specials who have not changed their passwords.” You can view these reports interactively under ISPF, or run them automatically in batch.

Analyze SMF log files to create a comprehensive audit trail

Tivoli zSecure Audit analyzes SMF from the live SMF data sets or from extracted SMF data on tape or disk. The SMF analysis component supports more than 40 standard z/OS SMF record types and includes specific auditing functions for RACF, ACF2, TSS, DB2 and UNIX, to produce overview and detail reports about system and user activity from the SMF log files. On z/OS systems with TSS, the Audit Tracking File may also be used.

By using live data sets, information from the active system can immediately be viewed interactively after an event has taken place. Tivoli 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 a comprehensive audit trail of a specific user ID from SMF, including events from SMF records that do not contain RACF information and events from batch jobs with arbitrary names.

Leverage external file support to make reports highly usable

Tivoli 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 it alongside the technical data from z/OS, RACF, ACF2 and TSS in automatically generated reports.

For example, if a policy exception takes place, such as logging in after work hours, then the information about the user (name, matching user ID, department, e-mail address and telephone details) is gathered from the personnel database.

Detect system changes to minimize security risks

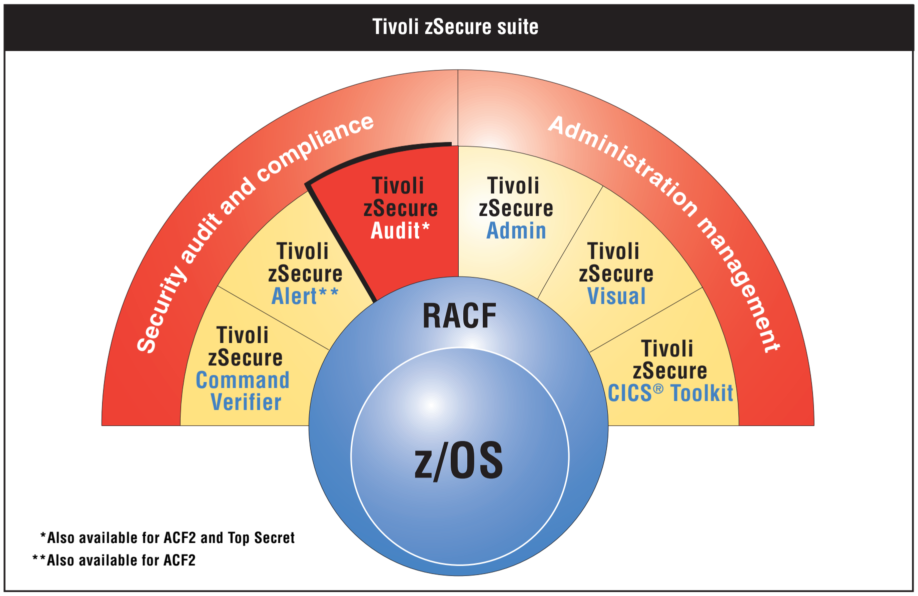
Tivoli zSecure Audit can identify changes in the individual members of partitioned data sets, using digital signatures for each member of the libraries under scrutiny. Tivoli zSecure Audit indicates whether a member was added, deleted or changed. For load modules, Tivoli zSecure Audit also identifies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

Tivoli 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. Tivoli zSecure Audit 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 may 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 Tivoli zSecure Command Verifier, which verifies each RACF command with your security policy and can stop noncompliant commands from being executed — before they do damage.

Tivoli zSecure suite


Security audit and compliance
Administration management
Tivoli zSecure Audit*
Tivoli zSecure Admin
Tivoli zSecure Alert**
Tivoli zSecure Visual
Tivoli zSecure Command Verifier
Tivoli zSecure CICS® Toolkit
RACF
z/OS

*Also available for ACF2 and Top Secret
**Also available for ACF2

Track and monitor baseline changes for RACF and ACF2

Tivoli zSecure Audit can help you define a baseline for RACF and ACF2 security parameters, as well as find indicators, such as profiles and parameters, that differ from the baseline. Changes in the indicators can be used to update the baseline, or can be tagged for follow-up. You can also add installation- and application-specific indicators to the baseline, such as profiles for application data sets, the mandatory inactivity of emergency user IDs or profiles accessible to specific users.

Detect integrity breaches

Tivoli zSecure Audit 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 to help you determine the type of corrective action that is needed.

Furthermore, Tivoli zSecure Audit integrates smoothly with IBM Tivoli zSecure

Tivoli zSecure Audit at a glance

System requirements:

- z/OS or z/OS.e

Supported administrative platforms:

- RACF
- CA ACF2
- CA Top Secret Security

Admin for end-to-end monitoring and remediation. Seamless integration with Tivoli zSecure Admin enables administrators to move quickly to diagnose and remediate failures or exposures.

Tivoli zSecure Audit can also integrate with IBM Tivoli Compliance Insight Manager so that you can incorporate mainframe security information into a broader enterprise audit and compliance solution.

For more information

Based on more than two decades of experience in security audit and compliance, Tivoli zSecure Audit offers an industry-leading solution to help organizations ease the burden of audit preparation and analysis. Tivoli zSecure Audit integrates seamlessly with the complete Tivoli zSecure suite of enterprise-wide security auditing solutions, providing a comprehensive, end-to-end workbench for RACF security management.

To learn more about how the Tivoli zSecure suite can help your organization meet audit challenges, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
6-07

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

TAKE BACK CONTROL WITH Tivoli