Auditing in a RACF Secured Environment

Document version 1.0

Ernie Mancill: mancill@us.ibm.com

Thomas Hubbard: thubbard@rocketsoftware.com

Kelly Smith: kelly.smith@rocketsoftware.com

CONTENTS

1 Premise: For some, the fact that DB2 on z/OS resides in a well protected RACF environment constitutes sufficient control and auditing is not required.

1.1 Summary:

- RACF is the industry leading security product for z/OS and does an excellent job in protecting access to secured assets on DB2 on z/OS. However, it does little in the way of access and activity reporting. Audit Management Expert is an extremely robust tool which can collect and report on activity performed in DB2 on z/OS with relatively low overhead. It does not perform or enforce any security policies.

- In any well protected environment, users are required to possess special privileges, and the nefarious use of those privileges can allow for the access to sensitive data outside the well protected application environment. However, the legitimate access and use of these privileges are required by specific classes of users, such as database administrators (DBAs), in order to ensure the smooth operation and administration of the DB2 on z/OS environment.

- Understanding how trusted (privileged) users use special privileges to potentially access sensitive information is essential to ensuring that data is indeed protected. Robust auditing on the activities performed by privileged users, as well as the use of certain tools and SQL generation products is clearly needed. In addition, there must be documentation that the source of this audit data is clearly untainted, with no privileged user interference in the collection of audit data.

- Audit Management Expert provides the DB2 on z/OS customer an industrial strength auditing tool, with the ability to collect very granular levels of activity with relatively low overhead. Due to the nature of Audit Management Expert's architecture, organizations can demonstrate a clear separation of roles between the activities of the DBAs and the collection of audit data.

2 Protect or Audit?

The purpose of this document is to describe why, in an environment well protected by RACF, the requirement for robust auditing still exists. To begin, we need to define a couple of items. For the purposes of this discussion, RACF and its primary competitors CA-TopSecret™ and CA-ACF2™, are security products that provide access control and security functionality for the z/OS and z/VM operating systems. Included in these security products are interfaces that allow for the protection of DB2 for z/OS resources.
While there are some limited reporting capabilities within these security products, they are mainly limited to helping the security administrator with the task of maintaining the security environment, and are of limited value in forensic auditing.

The purpose of auditing is to ensure that the appropriate controls are in place to identify inappropriate access and use of production data. Although auditing does not enforce access patterns or implement security, it provides the forensic information used to analyze the activities of users after the access occurs. The key point to remember is that auditing solutions will do nothing to protect access to data or other DB2 resources.

Customers have historically been averse to performing auditing activities within the DB2 on z/OS environment for several reasons. These reasons include:

- The performance impact of auditing, as well as increased complexity in the management and operation of the DB2 environment.
- The sheer magnitude of audit information that can be collected when not properly filtered.
    - Auditors who make the request to "audit everything" soon become awash in a sea of audit data, while some of the audit data "wheat" is very interesting, it cannot be separated from the "chaff" of the unimportant and irrelevant.
    - Some customers believe that the simple retention of this "raw" audit data can demonstrate compliance. However, the absence of an easy to use reporting mechanism makes this saved data essentially unusable, and very few auditors possess the technical expertise to generate meaningful audit reports from this data.

To simplify the process of turning the sometimes massive amounts of audit data into meaningful and manageable information requires the introduction of easy to use audit management tools, such as the IBM Audit Management Expert for DB2 on z/OS.

2.1 The Privileged User Scenario

In order to ensure the continued health and well-being of any DBMS system, including DB2 and IMS on z/OS, there are many activities that must be performed on a regular basis by system and database administrators. These activities, while capable of being well controlled by external security processes such as RACF, are pervasive in effect, and can be used in ways that are contrary to security policies.

To site one possible scenario, there is sensitive data residing on a DB2 table, and the applications (CICS or IMS) which access this table are well protected by RACF. The DBA does not have RACF authority to execute the CICS application, but has DBADM authority to administer the table, and in many cases this includes SELECT authority. The DBA runs an UNLOAD utility against the table, extracting all of the data contained in the table and can then transfer that data through any number of mechanisms to an outside entity (FTP, Flash/USB, CSV to spreadsheet, etc). Since the user has special privileges against the table, there will be no evidence of a security violation as would be reported by RACF.

If, on the other hand, the environment was protected by the use of an auditing solution such as DB2 Audit Management Expert, there could be several different collection profiles in effect that would report on this authorized, but questionable, use of special privileges. One recommendation for audit collection is to monitor any SQL or Utility access for privileged users, conversely one could elect to monitor each utility event, and finally one could combine looking for one or both classes of events within a time interval. So, while it might be acceptable for the DBA to access the audited tables during normal business hours, auditing parameters might be set up to look for unusual access patterns outside of normal business hours.

The conundrum in all of this is that while these activities and the user permissions to them can be controlled, the nature of these authorities gives the privileged user capabilities to access DB2 and IMS resources and data by means outside the use of the well protected application environment. This has the affect of providing unlimited access to the data, and to a large extent, circumventing normal transaction level RACF protection.

2.2 Auditing the Privileged User

As discussed in the prior section, the privileged user needs special authorities and access to DB2 and IMS resources to effectively administer the DB2 and IMS in order to perform their job. In the absence of a robust auditing mechanism to monitor the use of special privileges and data access patterns performed by privileged users, it is impossible to trace when or if these special privileges have been abused.

In a DBMS environment where privileged user authorities have been granted, there must be some mechanism to track and record activities that are performed under the control of these privileged user identifiers. Audit Management Expert for DB2 and IMS are two solutions that help customers meet this requirement for robust auditing of DB2 and IMS activities.

2.3 Separation of Roles

Any mechanism used to audit activities of trusted users must be implemented in such a way as to prevent the privileged user from interfering with the collection or contaminating the source of the audit data. DB2 Audit Management Expert for z/OS maintains the necessary segregation of duties, resulting in assurance of audit data integrity, which results in more accurate reports. This allows DBAs to perform their own job duties and allows auditors to run audit reports independently of the DBAs, which results in easier and more accurate audits. Auditors now have the ability to adhere to published industry standards and external auditing without relying on the assistance of the personnel being monitored.

DB2 Audit Management Expert for z/OS is well-suited to enforce controls that govern DBAs as well as to report on their activity. DBAs must be trusted with sensitive data in order to do their jobs. Their responsibilities include maintaining, copying, and recovering sensitive data, as well as loading and reorganizing it. The continuous, automated auditing provided by DB2 Audit Management Expert for z/OS removes the opportunity to alter or even omit important data from the audit reports. Thus, an independent audit mechanism in place of personnel involvement provides assurance that reported data has not been modified. Consequently, the accuracy of data and reports is more reliable.

2.4 The solution using DB2 Audit Management Expert for z/OS[1]

Auditors using DB2 Audit Management Expert for z/OS do not need to go to a large number of sources to access data, nor do they need user IDs for DB2 or the operating system. They simply log into DB2 Audit Management Expert for z/OS to gain complete visibility of all auditable objects. An auditor can display collected data for all DB2 instances, or just the DB2 instances of interest, all from the central repository. The administration user interface, usually managed by the lead auditor, provides the ability to assign auditor's access to the tool, which in turn allows them access to the repository data. For these reasons, DB2 Audit Management Expert for z/OS makes auditing data much more manageable.

DB2 Audit Management Expert for z/OS collects audit data from several different sources, these can include the DB2 Audit Facility, the DB2 recovery log, and an optional SQL collection component called ASC (Audit SQL Collector). ASC provides the ability to collect more granular levels of audit details that are not available with the native DB2 Audit Facility. This additional level of detail, not provided with the native DB2 Audit Facility, can include all SQL events within each commit scope, and for dynamic SQL, the data values associated with each SQL statement. Audit events are combined and stored in a single relational repository to produce a complete view of this business activity for auditors.

There are several types of database events that can be tracked and audited. Some of these events include instances of denied access attempts without proper authorization, explicit grant and revoke statements, and the assignment and change of authorization IDs to access DB2. In addition, all selects (reads), all changes, and all create, alter, and drops are recorded when using ASC, providing the auditor with additional granularity of event data than can be collected by the native audit trace facility of DB2 for z/OS. In order to examine the effects of audited SQL statements, there is also an easy to use log analysis facility that provides the ability to see the before and after change records stored in the DB2 recovery log.

A centralized repository creates a single source for reporting, institutional controls, summarization of the data including high-level trending of audit anomalies and drill-down capability (one layer at a time), as well as a robust level of reporting events controlled by the auditor without DBA involvement. When audit data resides in a single audit repository on a separate DB2 with limited access privileges, you can further control access and better protect your audit data.

[1] For IMS customers, IMS Audit Management Expert provides similar auditing capability.

IBM United States of America
Produced in the United States of America

The e-business logo, the eServer logo, IBM, the IBM logo, OS/390, zSeries, SecureWay, S/390, Tivoli, DB2, Lotus and WebSphere are trademarks of International Business Machines Corporation in the United States, other countries or both.

Lotus, Lotus Discovery Server, Lotus QuickPlace, Lotus Notes, Domino, CA ACF2, Top Secret, and Sametime are trademarks of Lotus Development Corporation and/or IBM Corporation.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PAPER “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 states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

Information in this paper as to the availability of products (including portlets) was believed accurate as of the time of publication. IBM cannot guarantee that identified products (including portlets) will continue to be made available by their suppliers.

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

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
4205 South Miami Boulevard
Research Triangle Park, NC 27709 U.S.A.