IBM InfoSphere Guardium for z/OS

Helping to lower the costs and risks of compliance, security and audit—using proven z/OS technology.

Highlights

- Monitors and audits IMS, VSAM and DB2 on IBM z/OS activity by privileged users, mainframe-resident applications and network clients
- Provides visibility at a granular level into critical operations, including reads, data and structural changes
- Performs all analysis, reporting and storage of audit data off-mainframe in a secure environment
- Can be used for mainframe environments only, or deployed enterprise-wide to provide a unified security and compliance solution for both mainframe and distributed database environments
- Uses proven z/OS technology from IBM to maximize reliability and efficiency

Growing DB2 security and compliance requirements

Many organizations host extensive amounts of data in mainframe databases, which are sensitive and mission critical. Financial, personnel and customer records are among the information commonly found in these environments.

As a result, mainframe data is often within the scope of a growing range of compliance mandates. This is compelling organizations to implement new controls to ensure their IBM DB2®, IBM IMS™ and VSAM data is secure from unauthorized access and tampering by both internal and external parties, and that a detailed audit trail validating the effectiveness of the controls can easily be made available to auditors.

The IBM® InfoSphere® Guardium® solution offers a simple, yet powerful, means of securing critical data throughout the enterprise. It provides rapid, policy-based detection of anomalous activities that violate corporate policies; real-time responses, such as alerts; auditable workflow to ensure appropriate resolution of exceptions; and automated reporting capabilities, which simplify validation of compliance for mandates, such as SOX, PCI DSS and data privacy regulations.

The InfoSphere Guardium for z/OS® solution provides these capabilities for DB2, IMS and VSAM on z/OS. The solution can be used independently for the mainframe environment only, or integrated with other InfoSphere Guardium database security and monitoring components throughout the enterprise, to provide a secure, centralized audit repository and management point.

Avoid the security and cost issues associated with traditional solutions

Historically, organizations seeking to monitor and secure their sensitive data on z/OS have used custom-developed solutions based on logging utilities, such as trace or transaction logs. These solutions, and others built upon them, suffer from a variety of limitations, including:

- Reliance on mainframe DBAs for administration, thus failing to provide the separation of duties (SOD) required by auditors.
- Failure to capture all critical activities required by auditors (such as read operations when using Logging, or SQL statements when using Trace).
- Lack of granular analysis and alerting capability, eliminating the possibility of immediately detecting and containing important categories of unauthorized activities (such as an unauthorized update to data from a privileged user.)
- The need to apply significant amounts of skilled labor to maintain custom software or to analyze reports to detect policy violations.

InfoSphere Guardium for z/OS eliminates these limitations, while providing important additional capabilities, such as compliance workflow automation, reporting, and an enterprise-wide view of your database security and compliance posture.

Scalable enterprise-wide database security and compliance platform

InfoSphere Guardium for z/OS uses lightweight software probes, called S-TAPs, to capture DB2, IMS and VSAM activities by privileged users, mainframe-resident applications and network clients, including those connecting through services such as JDBC, DB2 or IMS Connect. Proven IBM event-capture technologies are used for each environment to ensure all critical operations are captured, without the use of Class 4 and Class 5 audit traces.

Each S-TAP on z/OS is designed for the unique monitoring requirements of a particular data environment. The IBM InfoSphere Guardium S-TAP for DB2 on z/OS module monitors all DB2 activities, including SELECTs, DML, data

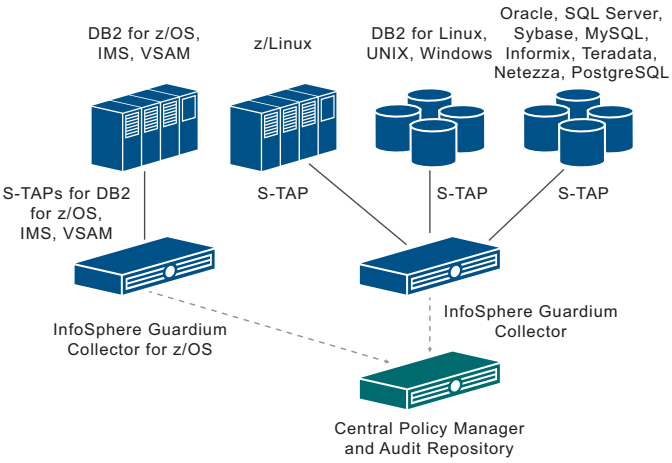

Figure 1: InfoSphere Guardium uses lightweight software probes to capture key DB2, IMS and VSAM activities executed by privileged users, mainframe-resident applications and network clients on z/OS. Both mainframe and distributed environments can be monitored from a single console; in addition, all audit data is automatically aggregated and normalized into a single centralized repository for enterprise-wide compliance reporting, analytics and forensics.

definition language (DDL) and changes in access privileges. To enhance performance, the underlying DB2 event-capture technology can be shared with IBM Query Monitor in systems utilizing both offerings. The IBM InfoSphere Guardium S-TAP for VSAM on z/OS module supports a comprehensive range of VSAM file types, including entry-sequenced data set (ESDS), key-sequenced data set (KSDS), relative record data set (RRDS), virtual relative record data set (VRRDS) and linear data set (LDS), monitoring OPENs, READs, UPDATEs, DELETEs, CREATEs and ALTERs. The IBM InfoSphere Guardium S-TAP for IMS on z/OS module monitors both online and batch tasks, providing auditing and policy management related to READs, INSERTs, UPDATEs, DELETEs.

Each S-TAP sends information specified by user-defined audit policies to an InfoSphere Guardium Collector for z/OS appliance. This ensures that the mainframe is not burdened with incremental storage or processing requirements, network traffic is limited, and a full audit trail is stored securely.

Timestamp	Client IP	Server IP	Server OS	DB User Name	OS User	Sql
2010-06-08 03:11:24.0	15:22:19.50	RL25	Z/OS	GU0002	GU0002	REVOKE EXECUTE ON PROCEDURE SYSTEM SQLTABLE PRIVILEGES FROM PUBLIC
2010-06-07 22:12:28.0	15:22:19.50	RL25	Z/OS	GU0001	GU0001	INSERT INTO udt_table VALUES(CAST(? AS udt1). CAST(? AS udt2). CAST(? AS udt3))
2010-06-08 03:04:29.0	15:22:19.50	RL25	Z/OS	GU0001	GU0001	INSERT INTO udt_table VALUES(CAST(? AS udt1). CAST(? AS udt2). CAST(? AS udt3))
2010-06-07 22:14:09.0	15:22:19.50	RL25	Z/OS	GU0001	GU0001	delete from camp_roster where NAME like?
2010-06-08 03:12:13.0	15:22:19.50	RL25	Z/OS	GU0002	GU0002	GRANT CREATIN, ALTERN, DROPIN ON SCHEME va_test_schema TO QA_TEST
2010-06-08 03:11:10.0	15:22:19.50	RL25	Z/OS	GU0002	GU0002	REVOKE EXECUTEMON PACKAGE NULLID,SYSSN101 FROM PUBLIC BY ALL
2010-06-08 02:29:05.0	15:22:19.50	RL25	Z/OS	GU0002	GU0002	GRANT ALL ON TABLE VA TEST, EMP TO VA TEST

Figure 2: InfoSphere Guardium provides comprehensive visibility into DB2, IMS and VSAM data usage on z/OS, capturing both mainframe and network access with key details such as OS user name, client IP, database user name and data access statements executed.

Unique in the industry, the InfoSphere Guardium multi-tier architecture aggregates and normalizes audit information—spanning database platforms, applications and locations—into a single centralized repository. This provides comprehensive enterprise-wide compliance reporting, correlation, forensics and database-focused analytics. Users starting with a mainframe implementation can scale up to support any mix of databases and systems—simply by adding appropriate S-TAPs, Collectors and Aggregators configured to work together in a federated model.

Automated, policy-based monitoring and auditing streamline compliance validation

The InfoSphere Guardium web console provides centralized management of alerts, report definitions, compliance workflow processes, and settings (such as archiving schedules) without the involvement of DBAs, thus providing the SOD required by auditors and streamlining compliance activities. A broad range of management functions can be executed across your entire database infrastructure, including:

- Defining granular access policies, using indicators of possible risk (appropriate for your particular environment), including data object, type of command, user ID, client IP address, OS user name, source application or time of day.
- Automatically creating a baseline of normal activities to suggest policies that will detect anomalous activities, such as SQL injection attacks.
- Defining actions in response to policy violations, such as generating alerts and logging full incident details.
- Automating compliance workflow for routine activities and incident responses, including steps such as sign-offs, commenting and escalation.
- Running hundreds of ready-to-use reports, including those required for SOX, PCI DSS and data privacy laws, in addition to creating customized reports.

With InfoSphere Guardium, you gain full visibility (see Figure 2) into your z/OS data environment, enabling unauthorized activities like data tampering or hacking to be identified and addressed in real time. Automation of the entire security and compliance life cycle reduces labor costs, facilitates communication throughout the organization, and streamlines audit preparation.

Comprehensive support for IBM environments

InfoSphere Guardium provides support for other popular IBM platforms, including:

- IBM DB2 for Linux, UNIX and Windows (LUW)
- IBM Informix
- IBM DB2 for iSeries®
- System z Red Hat Enterprise Linux and SUSE Linux Enterprise Server for System z, providing coverage for all major DBMS platforms (Oracle, MySQL and others) running in the IBM z/VM® hypervisor

IBM InfoSphere Guardium support for z/OS	
DB2 versions	DB2 for z/OS V8.1, V9.1, V10.1
IMS versions	V9, V10, V11, V12
z/OS versions	z/OS V1.10 (5694-A01) or later

Table 1: InfoSphere Guardium provides comprehensive z/OS support.

- Cognos®, for which the InfoSphere Guardium identifies fraud and other unauthorized activities through application-layer monitoring. InfoSphere Guardium solution also supports other enterprise applications, such as SAP, PeopleSoft and service-oriented architecture (SOA) applications developed for IBM WebSphere® Application Server and other middleware platforms

Why customers choose IBM InfoSphere Guardium solutions for System z

Customers choose IBM InfoSphere Guardium solutions for System z over the competition because:

- IBM has deep understanding of the System z mainframe environment with support for DB2 for z/OS, IMS, VSAM.
- Support for commercial and proprietary multi-vendor databases across a wide range of platforms as well as file stores and data streams such as Hadoop-based systems.
- Real-time alerts using low-latency, real-time streaming via TCP/IP.
- Does not require a DB2 repository—resulting in little interaction with the DBA for installation/configuration.
- User choice of IBM System z Integrated Information Processors (zIIP) for TCP/IP message processing and Stage 2 filtering.
- Simple and effective architecture for operational efficiency—one address space per DB2 subsystem.
- Single instance installation can take less than 30 minutes with 5 simple steps.
- Robust failover capabilities consistent with InfoSphere Guardium for Open Systems.
- Shared Collection approach running a single inspection process, reusable by multiple technologies and tools.
- Built-in tools, templates and mechanisms for assessing vulnerabilities, reporting, security, compliance, audit and automation.

Conclusion: Reduce your risk now

If you want to help lower risk by taking a proactive, preventative approach to audit, compliance and security—and would like to make security breaches a thing of the past—InfoSphere Guardium for System z can help protect all of an organization's data across a wide range of databases, transaction environments, and computing platforms. To learn more, visit **ibm.com/software/data/guardium**

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2012

IMD14429-USEN-00