

IBM Tivoli Compliance Insight Manager

Highlights

- Efficiently collect, store, investigate and retrieve logs through automated log management
- Perform privileged user monitoring and audit (PUMA) on databases, applications, servers and mainframes
- Help automate audit reporting through an enterprise compliance dashboard and flexible report distribution
- Create custom compliance modules through advanced policy and report definition engines
- Support auditing needs by translating captured native audit log data into easily understood language
- Ease addition of new log collectors and parsers through an advanced toolkit
- Leverage a full audit and compliance infrastructure through integration with numerous IBM Tivoli identity and access management products and advanced databases

Many businesses face the challenge of managing the massive amounts of log data that must be maintained for audit purposes. First, logs must be reliably and verifiably collected from dispersed sources across the enterprise, and done so in a continuous, sustainable manner. Once billions of log entries have been captured, a fast, efficient way to make sense of it all is needed.

Collecting and analyzing this information can take a significant amount of time and expertise. Many organizations — already stretched thin on resources — simply don't have the time and manpower. That's why there's IBM Tivoli® Compliance Insight Manager. An automated solution for monitoring, investigating and reporting on user activity across the enterprise, Tivoli Compliance Insight Manager can provide continuous, nonintrusive assurance and documentary evidence that your data and systems are being managed in accordance with company policies.

Quickly understand user activity through a comprehensive dashboard

Tivoli Compliance Insight Manager provides an easy-to-use security compliance dashboard that summarizes billions of log files. Through this dashboard, you can quickly gain an overview of your security compliance posture, understand user activities and security events in comparison to acceptable-use frameworks, and monitor privileged users and related security events.

Through its patent-pending W7 methodology, Tivoli Compliance Insight Manager translates native log data into easily understood language. A powerful combination, the W7 methodology and graphical dashboard can help you rapidly verify the seven W's: Who, did What, When, Where, Where from, Where to and on What.

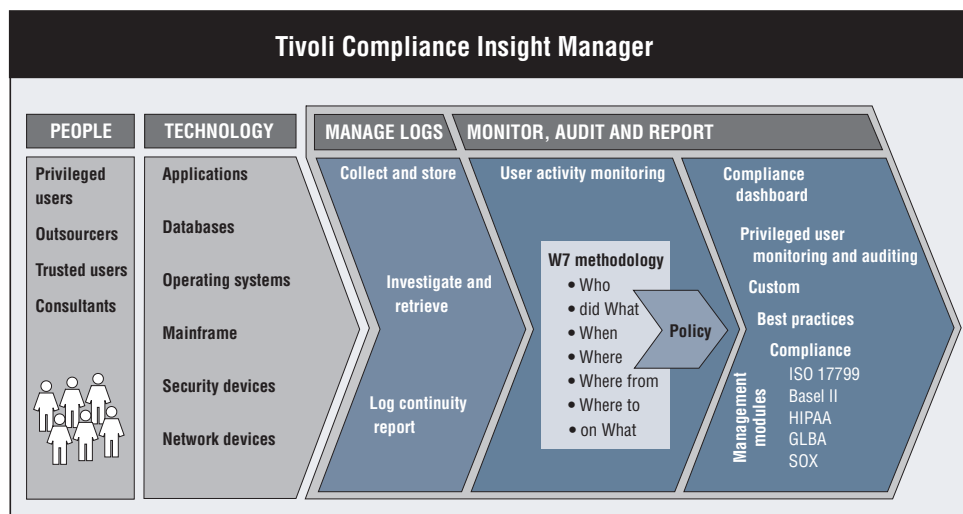
With this information at your fingertips, you can:

- Quickly drill down into user behavior, system activity and security information across all platform types.
- Compare log entries to baseline policy to help pinpoint and minimize security problems.
- Deliver reporting to support auditors' evidence requests and security managers' investigatory needs without burdening expensive subject matter experts.
- Rapidly respond to incidents through the ability to set actions and alerts about privileged user activity, while allowing administrators to perform their jobs.

Communicate audit and compliance information effectively and automate report distribution

Capturing and translating log data continuously and completely can significantly ease the burden of responding to compliance measures. Tivoli Compliance Insight Manager goes one step further by allowing organizations to instantly produce user- and data-oriented reports, along with customized and conditional reporting to meet specific reporting needs.

In addition, Tivoli Compliance Insight Manager offers more than 100 best-practice, audit and compliance-oriented reports to help address corporate and



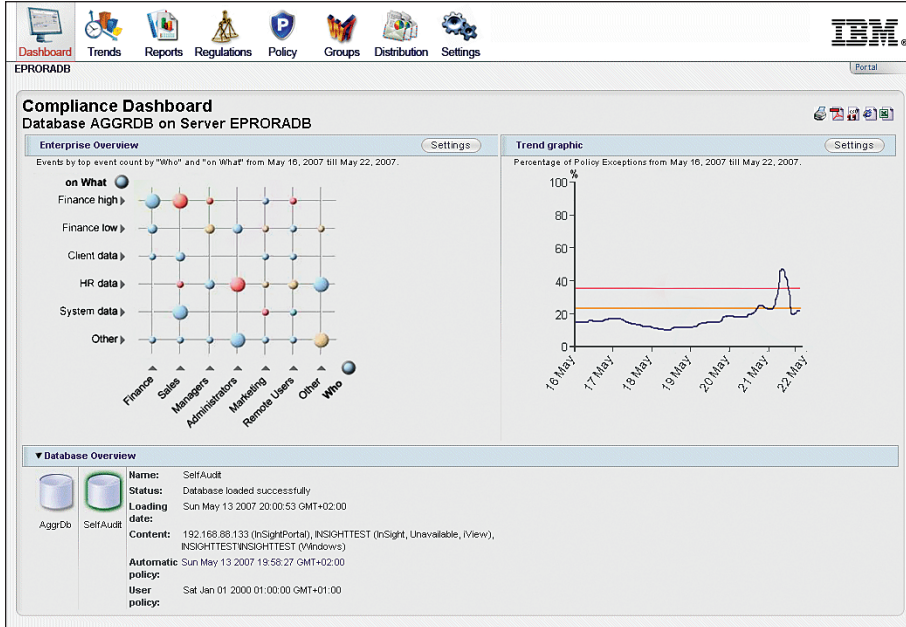
Tivoli Compliance Insight Manager captures security information about people and technology for audit and compliance reporting.

audit reporting requirements. Multiple templates — complete with a customizable acceptable-use policy that defines W7 groups and policies — help you jump-start the monitoring and reporting process. The automated policy generator aids you in establishing the baseline policies that can serve as the foundation for future investigations, and comparisons can be customized to help fit your organization's unique security policies.

And through the comprehensive audit and compliance dashboard, security managers can instantly view the compliance status of the organization, allowing them to pinpoint areas of concern and potential violations that require immediate investigation and remediation.

An automated report distribution facility enables you to easily define distribution lists of reports. These reports can then be sent to business owners for further verification or other action as required by your internal business processes.

Tivoli Compliance Insight Manager offers multiple Compliance Management Modules — specific to individual standards and regulations such as the Sarbanes-Oxley Act (SOX), International Organization for Standardization (ISO) 27001 and the Payment Card Industry Data Security Standard (PCI DSS) — that include specific targeted reports to help you monitor your compliance.



The Tivoli Compliance Insight Manager dashboard lets you quickly gain an overview of your security compliance posture, understand user activities and monitor privileged users in comparison to acceptable-use frameworks and security policy.

Create custom compliance modules through advanced policy and report definition engines

Tailoring your reporting requirements to meet the specific and detailed needs of your internal audit or compliance requirements can be a long, tedious process. The Tivoli Compliance Insight Manager custom reporting tool allows you to home in on specific reporting needs of your organization. The reports you create can also be distributed through the automated report distribution feature to allow integration into verification processes or other business workflows.

Capture data with automated enterprise log analysis

Most organizations have thousands of systems across the enterprise generating event logs, all of which must be captured and retained. Automating and centralizing the collection of log files can help make the process more efficient, saving time and money. Tivoli Compliance Insight Manager can help you securely and reliably collect, store, investigate and retrieve logs across the enterprise for compliance and investigative use.

A scalable log collector helps ensure the reliable and verifiable collection of native logs from virtually any

platform. And while many solutions only collect syslog and Simple Network Management Protocol (SNMP) logs, Tivoli Compliance Insight Manager captures much more and delivers:

- Operating system depth, including IBM System z,[™] IBM System i,[™] IBM AIX,[®] Sun Solaris, HP-UX, Microsoft[®] Windows[®] and Linux.[®]
- Audit trails from applications, whether written to a file or to a database table.
- Database depth for enhanced auditing capabilities, including integration with IBM DB2,[®] IBM Informix[®] Dynamic Server and Sybase ACE.
- Security device logs, through syslog and SNMP.
- Integration with numerous IBM Tivoli identity and access management products, such as IBM Tivoli Federated Identity Manager and IBM Tivoli Directory Server, to help you establish a full audit and compliance infrastructure.

To demonstrate to auditors and regulators the completeness and continuity of your log collection and management program, Tivoli Compliance Insight Manager offers a log continuity report.

Additionally, with optimized analysis tools, Tivoli Compliance Insight Manager can investigate and query suspected incidents through a compressed, long-term log depot. The log depot provides easy-to-use search capabilities to help you pinpoint potential security incidents.

Ease addition of new log collectors and parsers

An advanced toolkit in Tivoli Compliance Insight Manager simplifies the addition of new log collectors and parsers. These parsers can be used to define indexers that allow log data — collected from log files anywhere in the enterprise — to be included in searches in the depot investigation tool. This capability allows you to quickly perform queries that span all online log data. Consequently, you can get fast answers to enterprise incidents without having to resort to cumbersome, homegrown tools or highly technical query languages. Once incidents are identified, the original log data can be retrieved for use with additional forensic tools or platform-specific analysis tools.

Monitor and control the activities of privileged users

In the last few years, security risks posed by external sources have received significant media attention. While these high-profile attacks pose a very real threat to organizations, internal security incidents perpetrated by privileged users often pose an even greater threat. Whether inadvertent or malicious, the impact can include anything from lengthy outages to lost business to legal liability.

Tivoli Compliance Insight Manager enables you to monitor the activities of these powerful users so that you can verify that your policies are being enforced consistently — without limiting the ability of privileged users to do their jobs quickly and effectively.

When audit time rolls around, Tivoli Compliance Insight Manager can help you demonstrate to auditors that your organization:

- Logs and reviews systems administrator and systems operator activities on a regular basis.
- Analyzes and investigates security incidents and suspicious activity, plus takes remedial actions.
- Logs access to sensitive data, including root/administrator and database administrator (DBA) access.
- Continually maintains and reviews application, database, operating system and device logs.

Enhance IBM RACF auditing capabilities through plug-ins

Tivoli Compliance Insight Manager offers optional mainframe plug-ins with enhanced capabilities for RACF® auditing, helping reduce the cost and skill needed to maintain a secure environment for your business-critical assets. Designed to address the full range of RACF-specific security and compliance challenges, the plug-ins enable organizations to:

- Quickly analyze and report on mainframe events.
- Automatically detect security exposures through extensive status auditing.
- Create standard and customized reports that can be generated in XML format for use in databases and reporting tools.
- Quickly determine unauthorized logons and attempts, user behavior that violates security policy and when core systems are at risk.
- Verify RACF commands against your company's policies and procedures, and block or fix the ones that don't comply.

Integrate with security event management, identity management and access control solutions

Tivoli Compliance Insight Manager complements IBM Tivoli Security Operations Manager to help organizations improve incident response and policy compliance.

By sending information about critical events from Tivoli Compliance Insight Manager to Tivoli Security Operations Manager, security operations personnel can take immediate action. Tivoli Security Operations Manager can also provide policy violation data to Tivoli Compliance Insight Manager. For example, Tivoli Security Operations Manager can send exception data to Tivoli Compliance Insight Manager if incident response times exceed company policy, thus allowing security

personnel to investigate these exceptions before they can threaten security or compliance measures.

Additionally, Tivoli Compliance Insight Manager integrates with IBM Tivoli Identity Manager, IBM Tivoli Access Manager for e-business and IBM Tivoli Access Manager for Operating Systems. This integration allows you to monitor administrative activity on these servers to determine whether changes and activity by Tivoli Identity Manager and Tivoli Access Manager administrators occur within your policy and acceptable-use guidelines. Tivoli Compliance Insight Manager also integrates with the administrator directories of Tivoli Identity Manager and Tivoli Access Manager software so that administrative users' actual user names are included in Tivoli Compliance Insight Manager reports.

For more information

Based on more than two decades of experience in security audit and compliance management, Tivoli Compliance Insight Manager offers a leading solution for log analysis, privileged user monitoring, and audit and compliance reporting across the entire enterprise — from operating systems and applications to databases, mainframes and network devices.

Tivoli Compliance Insight Manager at a glance

Minimum enterprise server requirements:

- 4x Intel® Xeon® 3.0GHz processor
- 6GB RAM
- Windows 2000 Advanced Server SP4 or Windows 2003 Server SP1
- Microsoft Internet Explorer® 6.0 and above for viewing HTML reports

Minimum standard server requirements:

- 2x Xeon 3.0GHz processor
- 4GB RAM
- Windows 2000 Advanced Server SP4 or Windows 2003 Server SP1
- Microsoft Internet Explorer 6.0 and above for viewing HTML reports
- Syslog-NG 1.6.6 and later

Specific requirements will depend on log volumes and types of log data. The items listed above represent minimum requirements.

To learn more about how Tivoli Compliance Insight Manager can help your organization monitor user activity and integrate compliance efforts, contact your IBM representative or IBM Business Partner, or visit ibm.com/tivoli

About Tivoli software from IBM

Tivoli software provides a set of offerings and capabilities in support of IBM Service Management, a scalable, modular approach used to deliver more efficient and effective services to your business. Helping meet the needs of any size business, Tivoli software enables you to deliver service excellence in support of your business objectives through integration and

automation of processes, workflows and tasks. The security-rich, open standards-based Tivoli service management platform is complemented by proactive operational management solutions that provide end-to-end visibility and control. It is also backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli customers and business partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world — visit www.tivoli-ug.org



© Copyright IBM Corporation 2007

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

Produced in the United States of America
December 2007
All Rights Reserved

AIX, DB2, IBM, the IBM logo, Informix, RACF, System i, System z and Tivoli are trademarks of International Business Machines Corporation in the United States, other countries or both.

Intel and Xeon are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Internet Explorer, Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries or both.

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

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 

TID10355-USEN-01