

Deploy next-generation mainframe security administration, compliance and audit solutions.



Highlights

- Facilitate compliance with security requirements
- Leverage seamless integration with an enterprise-wide view of audit and compliance efforts
- Monitor and audit incidents to help not only detect but also prevent security exposures
- Automate routine administrative tasks to help reduce costs and help improve productivity

Help minimize risk and increase efficiency with the IBM Tivoli zSecure suite

Every organization has a core set of mission-critical data that must be protected. Security lapses and failures are not simply disruptions — they can be catastrophic events, and the consequences can be felt across the entire organization. The inadvertent mistakes of privileged users alone can result in millions of dollars in damages through unintentional configuration errors and careless security commands. Malicious users with authorized access can cause even greater damage.

As a result, security administrators face serious challenges in protecting the company's sensitive data. IT staff are challenged to provide detailed audit and controls documentation at a time when they're already facing increasing

demands on their time, due to events such as mergers, reorganizations and other changes. Many organizations do not have enough experienced mainframe security administrators to meet demand, and expanding employee skillsets with low-level mainframe security technologies can be time-consuming.

One way to offset these challenges is to establish effective processes to manage user administration, audit configurations and settings, and monitor changes and events. That's where the IBM Tivoli® zSecure suite comes in. This comprehensive suite can help enhance the security of mainframe systems by automating administration and audit processes — and ease the burden of compliance measures along the way.

Help increase security and decrease complexity

The Tivoli zSecure suite consists of multiple modular components designed to help you administer your mainframe security server, monitor for threats, audit usage and configurations, and enforce policy compliance.

Administration, provisioning and management components can significantly reduce administration, contributing to improved productivity, faster response time and reduced training time needed for new administrators. These offerings include:

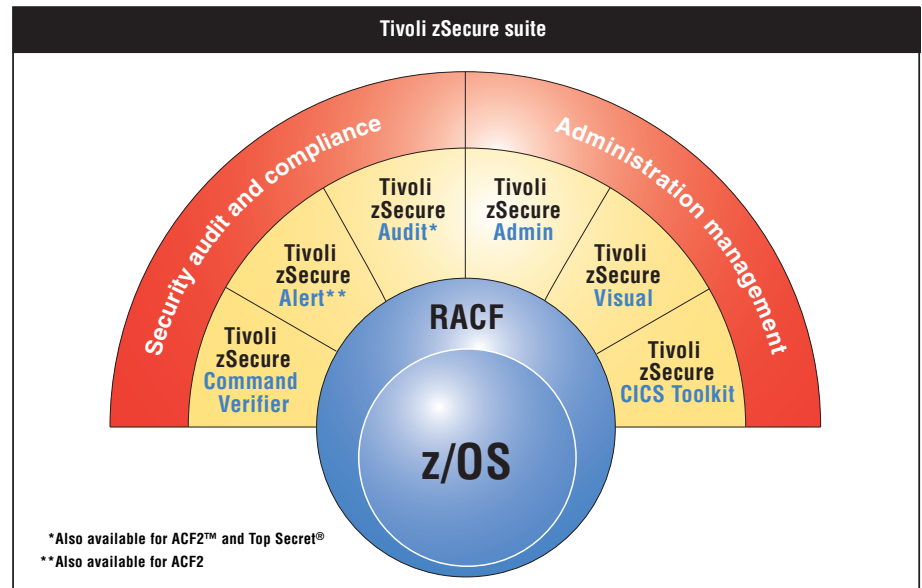
- IBM Tivoli zSecure Admin.
- IBM Tivoli zSecure Visual.
- IBM Tivoli zSecure CICS® Toolkit.

Audit, monitoring and compliance

components help ease the burden of compliance audits, improve security and incident handling, and increase overall operational effectiveness. Offerings include:

- IBM Tivoli zSecure Audit.
- IBM Tivoli zSecure Alert.
- IBM Tivoli zSecure Command Verifier.

In addition, the Tivoli zSecure suite also allows you to feed mainframe security



information into an enterprise audit and compliance solution, through seamless integration with IBM Tivoli Compliance Insight Manager. Combining mainframe data with that from other operating systems, applications and databases, Tivoli Compliance Insight Manager provides the unique ability to capture comprehensive log data, interpret that data through sophisticated log analysis and communicate results in an efficient, streamlined manner for full enterprise-wide audit and compliance reporting.

Help free administrators to focus on security

While preventing security breaches is paramount, administrators are frequently bogged down with tedious,

time-consuming day-to-day tasks that can divert their attention from security issues. The Tivoli zSecure suite offers a range of products designed to help reduce administration time, enabling valuable mainframe resources to focus on improving security quality.

Tivoli zSecure Admin is a leading security software product that enables efficient and effective IBM Resource Access Control Facility (RACF®) administration to help improve productivity. By putting a user-friendly layer over your RACF databases, you can more quickly enter and process administrative commands, generate custom reports and clean up databases. And by implementing a repeatable process

for security management, Tivoli zSecure Admin can help you reduce errors and improve the overall quality of services.

Tivoli zSecure Visual can reduce the need for expensive, RACF-trained expertise through a Microsoft® Windows®-based GUI for RACF administration. With the ability to establish a secure connection directly with RACF, Tivoli zSecure Visual is ideal for decentralizing RACF administration, without requiring green-screen (3270) or ISPF/TSO skills for security administration.

Tivoli zSecure CICS Toolkit allows you to perform mainframe administrative tasks from a Customer Information Control System (CICS) environment, helping free scarce native-RACF resources from basic administrative routines and enabling decentralized administration.

Track security events and prevent exposures to address compliance

Keeping up with the demands for audit and controls documentation — while also trying to prevent security breaches — can be overwhelming. The Tivoli zSecure suite delivers auditing, monitoring and compliance solutions designed to help reduce

security exposures while helping minimize the time needed to comply with auditors' requests.

Tivoli zSecure Audit delivers a comprehensive mainframe compliance and audit solution that enables you to quickly analyze and report on mainframe events, and automatically detect security exposures through extensive status auditing. The technology lets you create standard and customized reports that can be viewed under ISPF/TSO or generated in Extensible Markup Language (XML) format for use in databases and reporting tools. 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.

Tivoli zSecure Alert offers a real-time mainframe threat monitoring solution that allows you to efficiently monitor intruders and identify misconfigurations that could hamper your compliance efforts. It goes beyond conventional intrusion detection solutions to support intrusion prevention, by taking countermeasures via automatically generated commands. In addition, Tivoli zSecure Alert enables you to quickly determine

unauthorized logons and attempts, user behavior that violates security policy and instances where your core systems are at risk. With this information readily in hand, you can help identify misconfigurations before they can be exploited, while staying one step ahead of the auditors.

Tivoli zSecure Command Verifier is a robust policy enforcement solution that adds granular controls for keywords and parameters in RACF commands, and can help enforce mainframe compliance to company and regulatory policies by helping prevent erroneous commands. As a result, it helps increase control and decrease security risks and cleanup costs. Running in the background, Tivoli zSecure Command Verifier checks RACF commands against your company's policies and procedures. When commands are entered, it verifies whether the commands comply with security policies — and blocks or optionally adjusts the ones that don't.

Bringing it all together

The Tivoli zSecure suite is a valuable part of managing mainframe security as a process that meets the needs of regulators, auditors and the business itself. These offerings are the product



of a 20-year commitment to innovation on the mainframe and to enabling you to improve and simplify mainframe security audit and administration.

Through a broad range of offerings, the Tivoli zSecure suite helps you address your key challenges:

- Audit and compliance:
 - Report on questionable system options and dangerous settings of privileged users.
 - Measure and verify the effectiveness of mainframe security and security policies.
 - Generate alerts with instant reports about RACF, IBM System Management Facilities (SMF), IBM z/OS®, IBM DB2® and the UNIX® subsystem.
- User and security administration:
 - Centrally manage and provision users, profiles and resources.
 - Constantly monitor crucial users and information for misuse.
 - Help reduce operational costs and achieve fast incident detection.

For more information

To learn more about how the Tivoli zSecure suite can help your organization meet its mainframe security administration and audit

challenges, contact your IBM representative or IBM Business Partner, or visit ibm.com/tivoli

About Tivoli software from IBM

Tivoli software provides a comprehensive 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. Meeting 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 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
6-07
All Rights Reserved

CICS, DB2, IBM, the IBM logo, RACF, Tivoli and z/OS are trademarks of International Business Machines Corporation in the United States, other countries or both.

ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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 