Tivoli software

IBM Tivoli zSecure Command Verifier

Highlights

- Proactively enforce policy compliance on IBM RACF
- Help decrease database pollution by preventing noncompliant RACF commands
- Conserve resources by helping eliminate RACF cleanup time and reducing audit concerns
- Help reduce the risk of security breaches and failed audits caused by internal errors and noncompliant commands
- Receive alerts when risky commands are executed to help reduce chances of outages

Central administrators of Resource Access Control Facility (RACF®) mainframes often find themselves plagued with problems caused when technical specialists, field administrators, help-desk users, application security administrators and other decentralized administrators issue commands that are not compliant with security policies. Mistakes and ignored procedures, such as naming standards and standards for granting authorities, result in a "polluted" mainframe environment that may require countless hours to clean. Worse, they can leave your infrastructure open to vulnerabilities and serious audit concerns.

Left unattended, a database that is inconsistent and poorly structured with noncompliant commands can lead to:

- Violations of your naming standards and installation policies.
- Profiles that are put into warning mode.
- Outages.
- Audit findings and failed audits.

Central mainframe administrators need a way to prevent changes that can reduce the availability and compliance of their systems, cause database pollution or increase policy violations and security vulnerabilities. IBM Tivoli® zSecure Command Verifier takes control of RACF commands so you can ensure the security of your RACF mainframe environment.

Tivoli zSecure Command Verifier acts as a filter for RACF commands as they are entered, by intercepting commands, comparing them to your security policy and then determining whether or not they should be executed. In effect, Tivoli zSecure Command Verifier provides an additional security layer that enables you to compare each RACF command to your security policies, prior to processing. These policy rules are defined through normal RACF profiles, so security specialists do not require programming

skills or assembler coding knowledge to configure Tivoli zSecure Command Verifier. Tivoli zSecure Command Verifier enables you to:

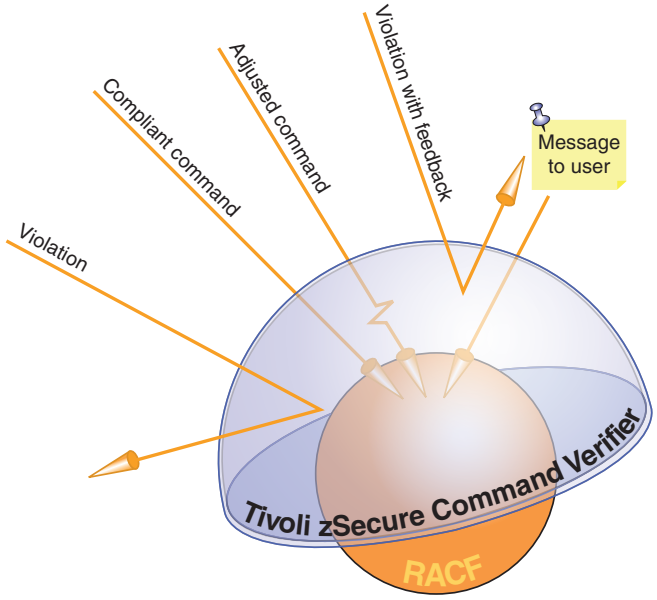
- Conserve resources by eliminating RACF cleanup time.
- Reduce the risk of security breaches and failed audits.
- Increase security control, even when decentralizing administration.
- Audit policy definitions with normal RACF reporting procedures.

Verify commands before processing to proactively monitor policy compliance

Tivoli zSecure Command Verifier helps prevent noncompliant administrative commands from being executed. For instance, in a RACF environment, privileged users may be able to change or delete all profiles within their scope — or violate your installation policies for applications and devices.

To help prevent these kinds of security violations, Tivoli zSecure Command Verifier automatically verifies command keywords against your specified policies as soon as a RACF command is issued — regardless of how it is initiated — whether from Time Sharing Option (TSO), Interactive System Productivity Facility (ISPF), batch jobs or the operator console. Among other capabilities, Tivoli zSecure Command Verifier lets you:

- Limit authorities on select profiles to READ.
- Require the use of GROUPs on the PERMIT command.
- Enforce naming conventions.
- Prevent changes to SETROPTS options.
- Enforce application installation policies.



Tivoli zSecure Command Verifier acts as a protective shield against noncompliant commands to the RACF mainframe environment.

Retrieve command information effortlessly with Command Audit Trail feature

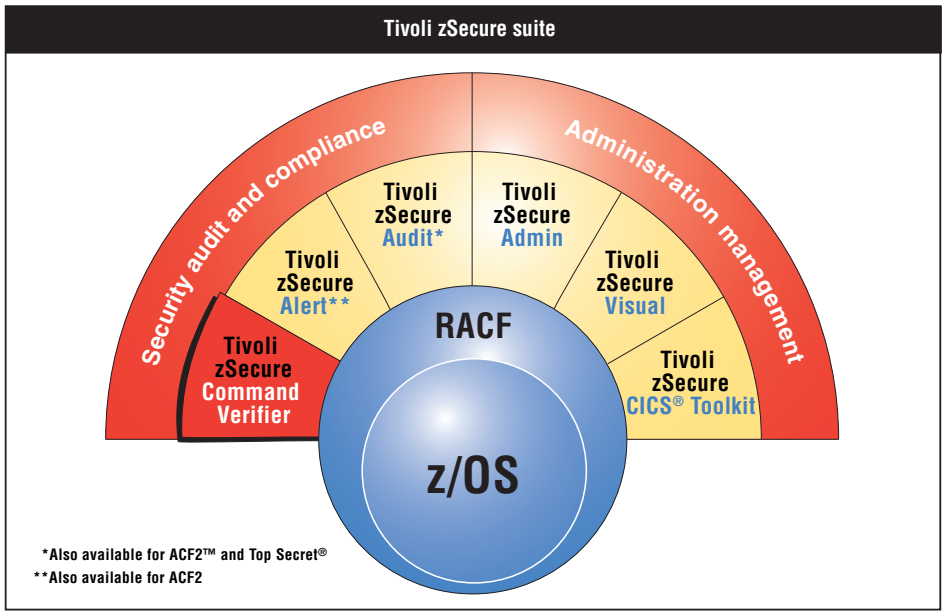
A special Command Audit Trail feature in Tivoli zSecure Command Verifier stores changes to profiles in the RACF database, so you can easily discover when a change to a profile was made and which administrator issued a particular command. This can save you countless hours of going back into log files, guessing the timeframes and searching for the information. With the Command Audit Trail feature, you can retrieve this information in seconds.

Take control by setting policies, alerts and default values

To help you stay ahead of — and prevent — potential security breaches, system administrators can easily use Tivoli zSecure Command Verifier to specify policies via RACF profiles and to determine the type of verification to be performed and any actions to take if the command is not compliant.

In addition, Tivoli zSecure Command Verifier can generate immediate, real-time alerts if critical RACF commands are issued, helping to prevent system outages caused when administrators issue incorrect RACF commands.

You can also establish policy definitions to provide mandatory and default values for commands for which RACF does not provide appropriate defaults. In addition, Tivoli zSecure Command Verifier enables you to grant users access to specific commands that they would not normally be authorized to use. This capability is typically used to authorize help-desk personnel to display users, groups and resource definitions. By using these convenient, automated control features, Tivoli zSecure Command Verifier helps central administrators to protect RACF security.



Easy, independent installation to help speed time to value

Because Tivoli zSecure Command Verifier is implemented as part of the RACF Common Command Exit — a standard RACF application programming interface (API) — it helps eliminate the need to design, code and maintain assembler routines that handle parsing of hundreds of keywords. Because the software runs as a command exit, it should be installed on all systems for which your installation policies must be enforced. Tivoli zSecure Command Verifier works independently of the other solutions in the Tivoli zSecure suite and can serve as an important add-on to other third-party RACF tools that lack this vital functionality.

Leverage the Tivoli zSecure product family

Tivoli zSecure Command Verifier is part of the family of Tivoli zSecure products designed to provide comprehensive audit and administration process automation for the mainframe. The robust security features in the Tivoli zSecure product family represent the IBM commitment to delivering the industry's best security interface for your mainframe.

Tivoli zSecure Command Verifier at a glance

System requirements:

- IBM z/OS® or z/OS.e

Supported administrative platform:

- RACF

For more information

For more information about how Tivoli zSecure Command Verifier can help you proactively monitor commands sent to the RACF mainframe environment, 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

TAKE BACK CONTROL WITH Tivoli®

TID10403-USEN-00