**Durchsetzen von RACF-Richtlinien und Schutz der Sicherheit Ihrer Großrechnerumgebung**

Tivoli® software

# IBM Tivoli zSecure Command Verifier

## Highlights

- Proaktive Sicherstellung der Richtlinienkonformität auf IBM RACF
- Geringere „Verunreinigung" von Datenbanken durch Verhinderung der Ausführung gegen Richtlinien verstoßender Befehle
- Einsparung von Ressourcen durch Eliminierung der Zeit für die RACF-Bereinigung und durch Reduzierung von Prüfproblemen
- Reduzieren des Risikos von Sicherheitsverstößen und des Fehlschlagens von Prüfungen aufgrund interner Fehler und den Richtlinien widersprechender Befehle
- Versenden von Benachrichtigungen, wenn risikoträchtige Befehle ausgeführt werden, um so mögliche Ausfallzeiten zu verringern

Zentrale Administratoren von RACF-Mainframe-Computern (Resource Access Control Facility) stehen oft vor erheblichen Problemen, die dadurch verursacht werden, dass Techniker, lokale Administratoren, Help-Desk-Benutzer, für die Anwendungssicherheit zuständige Administratoren und weitere dezentrale Administratoren Befehle ausgeben, die den Sicherheitsrichtlinien widersprechen. Fehler und die Missachtung von Vorgehensweisen, etwa von Benennungsstandards oder von Standards für die Zuweisung von Berechtigungen, führen zu einer „verunreinigten" Großrechnerumgebung, deren Bereinigung zahllose Stunden in Anspruch nehmen kann. Schlimmer noch: Derartige Probleme können dazu führen, dass Ihre Infrastruktur Sicherheitslücken aufweist und erhebliche Prüfprobleme verursacht.

Wenn Sie sich nicht um eine inkonsistente und schlecht strukturierte Datenbank, die Richtlinien widersprechende Befehle enthält, kümmern, kann dies zu folgenden Problemen führen:

- *Verletzungen Ihrer Benennungsstandards und Installationsrichtlinien*
- *Profile, die in den Warnmodus gesetzt werden*
- *Ausfallzeiten*
- *Beanstandungen durch Prüfungen und fehlgeschlagene Prüfungen*

Zentrale Mainframe-Administratoren müssen Änderungen verhindern können, die die Verfügbarkeit und die Richtlinienkonformität ihrer Systeme beeinträchtigen, die „Verunreinigungen" von Datenbanken verursachen oder Richtlinienverletzungen und Sicherheitsrisiken erhöhen können. IBM Tivoli zSecure Command Verifier kontrolliert die RACF-Befehle, so dass Sie die Sicherheit Ihrer RACF-Großrechnerumgebung sicherstellen können.

Tivoli zSecure Command Verifier fungiert als Filter für RACF-Befehle bei ihrer Eingabe. Die Lösung fängt Befehle ab, vergleicht sie mit Ihrer Sicherheitsrichtlinie und entscheidet dann, ob sie ausgeführt werden sollen oder nicht. Tatsächlich bietet Tivoli zSecure Command Verifier eine zusätzliche Sicherheitsebene, mit deren Hilfe Sie jeden RACF-Befehl vor seiner Verarbeitung mit Ihren Sicherheitsrichtlinien abgleichen können. Diese Richtlinien werden durch normale RACF-Profile definiert, so dass Sicherheitsspezialisten nicht über Programmier- oder Assemblercode-Kenntnisse verfügen müssen, um Tivoli zSecure Command Verifier zu konfigurieren. Tivoli zSecure Command Verifier bietet folgende Vorteile:

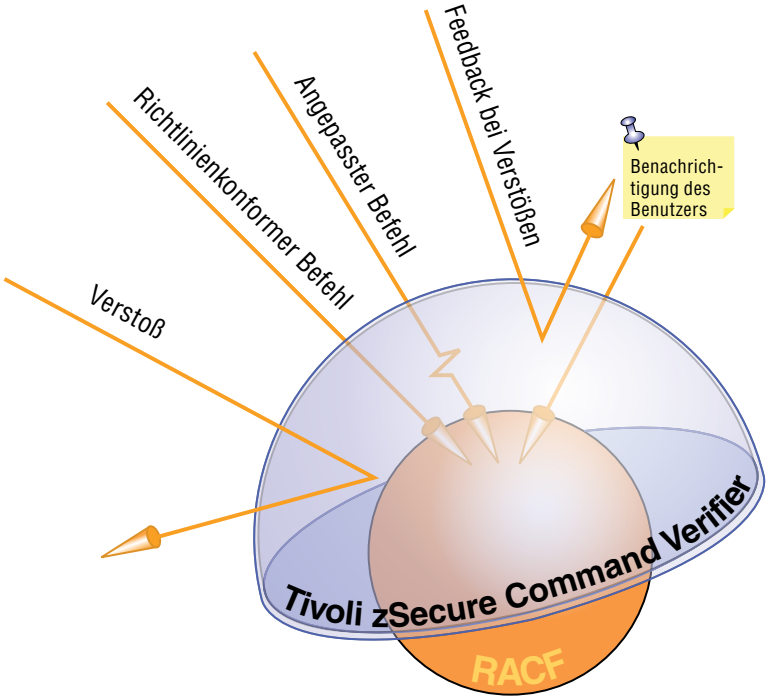
- *Einsparung von Ressourcen durch Eliminierung der Zeit für die RACF-Bereinigung*
- *Reduzierung des Risikos von Sicherheitsverletzungen und fehlgeschlagenen Prüfungen*
- *Verbesserung der Sicherheitssteuerung, auch bei dezentralisierter Verwaltung*
- *Prüfung von Richtliniendefinitionen mit normalen RACF-Berichtsverfahren*

**Überprüfung von Befehlen vor ihrer Verarbeitung zur proaktiven Überwachung der Richtlinienkonformität**

Mit Tivoli zSecure Command Verifier können Sie die Ausführung von Verwaltungsbefehlen verhindern, die bestehenden Richtlinien widersprechen. So ist es beispielsweise möglich, dass privilegierte Benutzer in einer RACF-Umgebung alle Profile in ihrem Bereich ändern oder löschen – oder Ihre Installationsrichtlinien für Anwendungen und Geräte verletzen können.

Zur Verhinderung derartiger Sicherheitsverstöße überprüft Tivoli zSecure Command Verifier automatisch Befehlsschlüsselwörter anhand von Ihnen festgelegter Richtlinien, sobald ein RACF-Befehl ausgegeben wird. Dies geschieht unabhängig davon, wie er initiiert wurde, ob von Time Sharing Option (TSO), von Interactive System Productivity Facility (ISPF), von Stapeljobs oder über die Bedienerkonsole.
Tivoli zSecure Command Verifier bietet unter anderem folgende Möglichkeiten:

- *Beschränkung der Berechtigungen auf READ für ausgewählte Profile*
- *Durchsetzung der Verwendung von GROUPs für den PERMIT-Befehl*
- *Erzwingung von Namenskonventionen*
- *Verhinderung von Änderungen an SETROPTS-Optionen*
- *Durchsetzung von Richtlinien für die Anwendungsinstallation*




*Tivoli zSecure Command Verifier fungiert als Schutzschild gegen Befehle an die RACF-Großrechnerumgebung, die gegen Richtlinien verstoßen.*

**Problemloser Abruf von Befehlsinformationen mittels der Funktion Command Audit Trail**

Die spezielle Funktion Command Audit Trail in Tivoli zSecure Command Verifier speichert Änderungen an Profilen in der RACF-Datenbank. So können Sie leicht erkennen, wann ein Profil geändert wurde und welcher Administrator einen bestimmten Befehl ausgegeben hat. So sparen Sie möglicherweise endlose Stunden, die Sie ansonsten mit der Überprüfung von Protokolldateien, der Schätzung der Zeiträume und der Suche nach Informationen verbringen müssten. Mit der Funktion Command Audit Trail können Sie diese Informationen in wenigen Sekunden abrufen.

**Übernehmen Sie die Kontrolle durch Festlegung von Richtlinien, Benachrichtigungen und Standardwerten**

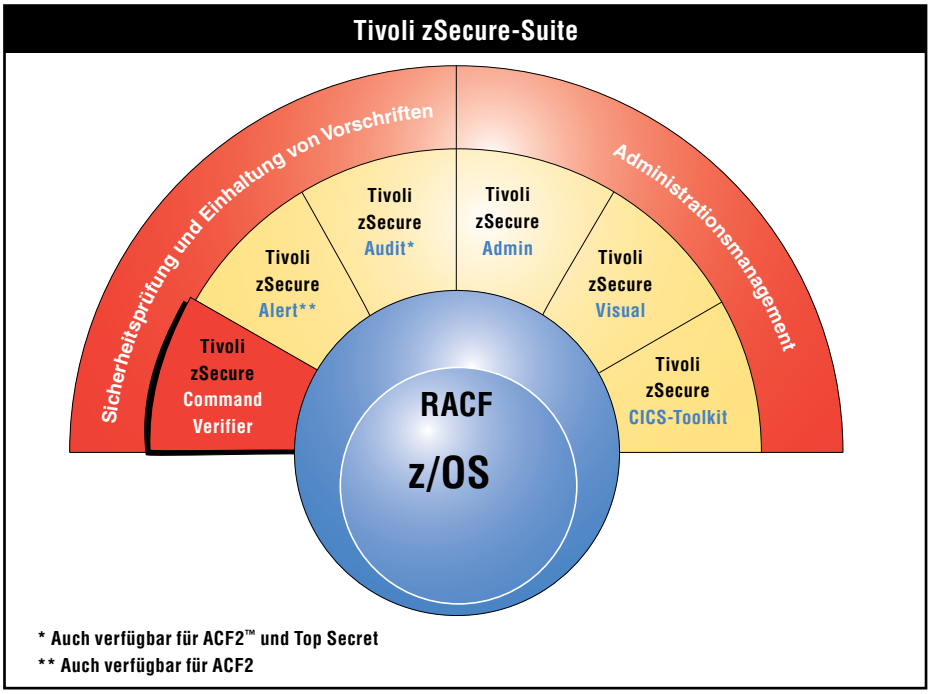
Damit Sie potenzielle Sicherheitsverstöße beherrschen – und verhindern – können, ermöglicht Tivoli zSecure Command Verifier Systemadministratoren die Angabe von Richtlinien über RACF-Profile und die Festlegung der durchzuführenden Überprüfungsaktionen sowie aller Maßnahmen, die erforderlich sind, wenn der Befehl die Richtlinien verletzt.

Darüber hinaus kann Tivoli zSecure Command Verifier sofortige Echtzeitbenachrichtigungen generieren, wenn kritische RACF-Befehle ausgegeben werden. Dies beugt Systemausfallzeiten vor, die entstehen können, wenn Administratoren inkorrekte RACF-Befehle ausgeben.

Ferner können Sie Richtliniendefinitionen einrichten, um obligatorische und standardisierte Werte für Befehle anzugeben, für die RACF keine geeigneten Vorgaben bietet. Zusätzlich ermöglicht Ihnen Tivoli zSecure Command Verifier, Benutzern den Zugriff auf bestimmte Befehle zu gewähren, die sie normalerweise nicht verwenden dürften. Diese Funktion wird üblicherweise dazu verwendet, Help-Desk-Mitarbeitern die Anzeige von Benutzern, Gruppen und Ressourcendefinitionen zu ermöglichen. Durch diese komfortablen, automatisierten Steuerfunktionen hilft Tivoli zSecure Command Verifier zentralen Administratoren beim Schutz der RACF-Sicherheit.

**Einfache, unabhängige Installation für kürzere Realisierungszeiten**

Da Tivoli zSecure Command Verifier im Rahmen von RACF Common Command Exit – eines Standard-RACF-API – implementiert wird, entfällt die Notwendigkeit, Assemblerroutinen zu entwerfen, zu kodieren und zu verwalten, die das Parsing von hunderten von Schlüsselwörtern leisten. Da die Software als Befehlsexit ausgeführt wird, sollte sie auf allen Systemen installiert werden, für die Ihre Installationsrichtlinien durchgesetzt werden müssen. Tivoli zSecure Command Verifier arbeitet unabhängig von den übrigen Lösungen der Tivoli zSecure-Suite und kann als wichtiges Zusatzprodukt zu RACF-Werkzeugen anderer Hersteller dienen, die nicht über diese wesentliche Funktion verfügen.




**Nutzen Sie die Tivoli zSecure-Produktfamilie**

Tivoli zSecure Command Verifier ist Teil der Tivoli zSecure-Produktfamilie, die umfassende Automatisierungsfunktionen für Prüfung und Verwaltung des Mainframe-Computers bietet. Die leistungsstarken Sicherheitsfunktionen der Tivoli zSecure-Produktfamilie unterstreichen das IBM Engagement für die Bereitstellung herausragender Sicherheitsschnittstellen für Ihren Mainframe-Computer.

**Weitere Informationen**

Wenn Sie mehr darüber erfahren möchten, wie Tivoli zSecure Command Verifier Ihnen dabei helfen kann, an die RACF-Großrechnerumgebung gesendete Befehle proaktiv zu überwachen, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter:

**ibm.com**/tivoli

## Tivoli zSecure Command Verifier auf einen Blick

**Systemvoraussetzungen:**

- IBM z/OS oder z/OS.e

**Unterstützte Verwaltungsplattform:**

- RACF

IBM Deutschland GmbH
70548 Stuttgart
**ibm.com**/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
**ibm.com**/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
**ibm.com**/ch

Die IBM Homepage finden Sie unter:
**ibm.com**



Gedruckt in den USA
06-07



*TAKE BACK CONTROL WITH* Tivoli

TID10403-DEDE-00