Vereinfachung der Sicherheitsprüfungen und der Überwachung privilegierter Benutzer mit einer leistungsfähigen Gesamtübersicht zur Richtlinieneinhaltung (Compliance Dashboard)

Tivoli software

IBM Tivoli Compliance Insight Manager

Highlights

- Automatisierung der Auditberichterstellung und der flexiblen Berichtsverteilung durch eine unternehmensweite Gesamtübersicht zur Richtlinieneinhaltung
- Professionelle Module zur Definition von Richtlinien und Berichten für die Erstellung kundenspezifischer Compliancemodule
- Unterstützung der Auditanforderungen durch Übersetzung der erfassten Audit-Logdaten in eine leicht verständliche Sprache
- Automatisiertes Log-Management zur effizienten Erfassung, Speicherung, Analyse und Abfrage von Logdaten
- Professionelles Toolkit für einfaches Hinzufügen neuer Komponenten zur Erfassung und Analyse von Logdaten
- Effektive Überwachung und Prüfung privilegierter Benutzer (Privileged-User Monitoring and Audit, PUMA) in Bezug auf Datenbanken, Anwendungen, Server und Großrechner
- Integration mit IBM Tivoli Identity Manager, IBM Tivoli Access Manager und IBM Tivoli Security Operations Manager, um die Maßnahmen zur Einhaltung von Vorschriften zu optimieren und auf Störungen zu reagieren

Viele Unternehmen sind gezwungen, gewaltige Mengen an Logdaten zu verwalten, die sie zu Auditzwecken behalten müssen. Zuerst müssen aus den verschiedensten Quellen im gesamten Unternehmen Logdaten erfasst werden, und das nicht nur zuverlässig und verifizierbar, sondern auch kontinuierlich und nachhaltig. Dabei reicht es nicht aus, Milliarden an Logeinträgen zu sammeln – es ist auch notwendig, dem Ganzen schnell und effektiv Sinn zu verleihen.

Die Erfassung und Analyse dieser Informationen kann mit einem beträchtlichen Aufwand an Zeit und Know-how verbunden sein. Viele Unternehmen – besonders wenn sie bereits ihre Ressourcen optimiert haben – verfügen einfach nicht über die notwendigen Kapazitäten an Zeit und Personal. Aus diesem Grund wurde IBM Tivoli Compliance Insight Manager entwickelt. Als automatisierte Lösung für die unternehmensweite Überwachung, Analyse und Dokumentation der Benutzeraktivität kann Tivoli Compliance Insight Manager kontinuierlich und unterbrechungsfrei gewährleisten, dass Ihre Daten und Systeme in Übereinstimmung mit den Unternehmensrichtlinien verwaltet werden, und ermöglicht den zugehörigen beleghaften Nachweis.

Umfassende, leicht verständliche Statusübersicht zur Benutzeraktivität

Tivoli Compliance Insight Manager stellt eine benutzerfreundliche Statusübersicht zur Einhaltung von Sicherheitsbestimmungen bereit, in der Milliarden an Logdateien in einer übersichtlichen Grafik zusammengefasst werden. Diese Statusübersicht gibt Ihnen schnell einen Überblick über den erreichten Stand in Bezug auf die Einhaltung von Sicherheitsbestimmungen; Sie werden über Abweichungen der Benutzeraktivität und sicherheitsrelevanter Ereignisse von definierten Rahmenbedingungen informiert und können privilegierte Benutzer und sicherheitsrelevante Ereignisse überwachen.

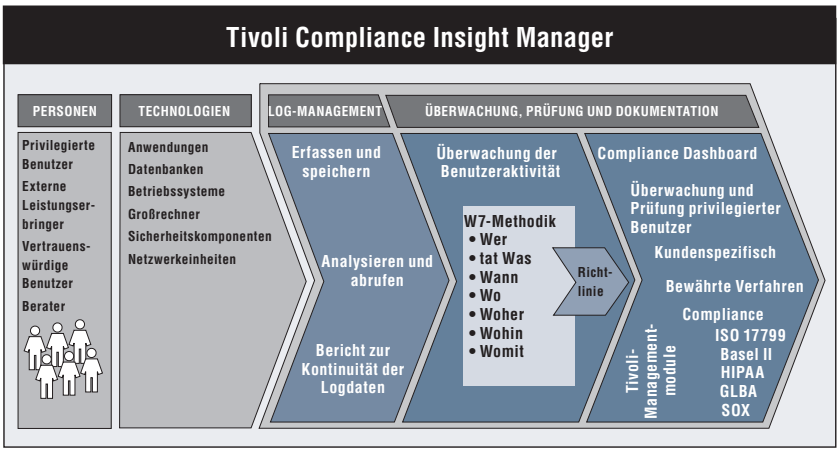
Mit einer eigenen, zum Patent angemeldeten W7-Methodik überträgt Tivoli Compliance Insight Manager originäre Logdaten in eine leicht verständliche Sprache. Die leistungsfähige Kombination aus W7-Methodik und grafisch orientierter Statusübersicht ermöglicht Ihnen die schnelle Verifizierung der sieben W's: Wer hat Was, Wann, Wo, Woher, Wohin und Womit getan.

Mit diesen Informationen können Sie:

- *Schnelle Detailabfragen/-analysen zu Benutzerverhalten, Systemaktivität und Sicherheitsinformationen für alle Plattformtypen durchführen.*
- *Logeinträge mit der Basisrichtlinie vergleichen, um Sicherheitsprobleme erkennen und minimieren zu können.*
- *Prüfern und Sicherheitsmanagern als Nachweis Berichte bereitstellen, ohne dazu eigens entsprechende Fachleute hinzuziehen zu müssen.*
- *Schnell auf Ereignisse reagieren, da die Möglichkeit besteht, spezielle Maßnahmen und Benachrichtigungen für privilegierte Benutzer festzulegen, ohne die Administratoren bei der Erfüllung ihrer Aufgaben zu behindern.*

Effektive Weitergabe von Audit- und Compliancedaten und Automatisierung der Berichtsverteilung

Durch die kontinuierliche und vollständige Erfassung und Übersetzung von Protokolldaten lässt sich der Aufwand für Gegenmaßnahmen bei Konformitätsverletzungen deutlich verringern. Tivoli Compliance Insight Manager geht aber noch weiter: Unternehmen können nicht nur unmittelbar benutzer- und datenorientierte Berichte, sondern auch angepasste und konditionale Berichte erstellen, um speziellen Anforderungen zu begegnen.

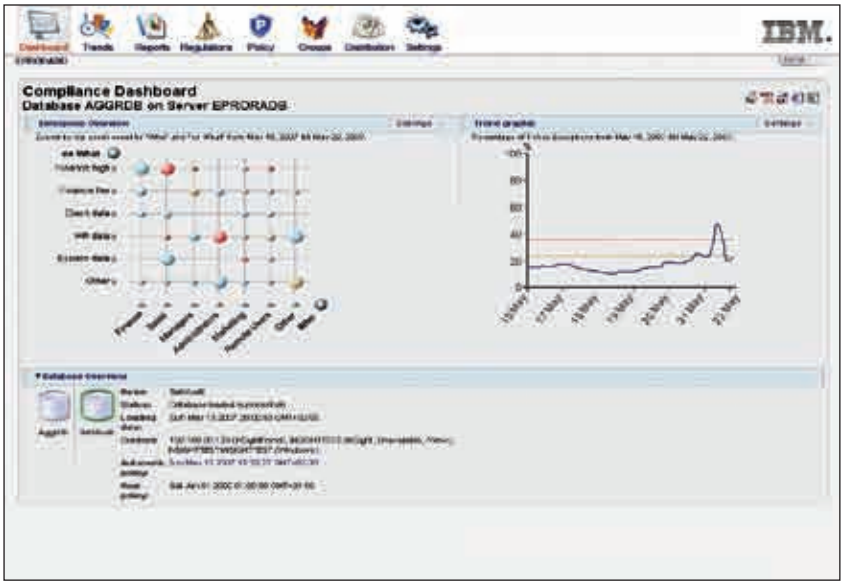


Tivoli Compliance Insight Manager erfasst Sicherheitsinformationen zu Personen und Technologien für Audit- und Complianceberichte.

Zusätzlich bietet Tivoli Compliance Insight Manager mehr als 100 bewährte Audit- und Complianceberichte für unternehmensinterne und -externe Audits. Viele Vorlagen – komplett mit einer anpassungsfähigen Nutzungsrichtlinie, die W7-Gruppen und -Richtlinien definiert – ermöglichen Ihnen einen schnellen Einstieg in den Prozess der Überwachung und Berichterstellung. Der automatisierte Richtliniengenerator unterstützt Sie bei der Entwicklung der Basisrichtlinien als Fundament für zukünftige Untersuchungen. Mit Hilfe von Vergleichen können Sie die einzigartigen Sicherheitsrichtlinien Ihres Unternehmens bedarfsgerecht zuschneiden.

Mit Hilfe der umfassenden Audit- und Compliance-Gesamtübersicht erhalten die Sicherheitsmanager in kürzester Zeit Einblick in die Richtlinienkonformität des Unternehmens und können so Problembereiche und potenzielle Verstöße erkennen, die eine unverzügliche Untersuchung und Korrektur erfordern.

Zusätzlich können Sie durch die automatisierte Berichtsverteilungsfunktion problemlos Verteilerlisten für Berichte definieren. Diese Berichte können dann je nach den Erfordernissen Ihrer internen Geschäftsprozesse entweder zur weiteren Prüfung an die Verantwortlichen geschickt oder für sonstige Maßnahmen genutzt werden.



Mit der Statusübersicht von Tivoli Compliance Insight Manager erhalten Sie schnell einen Überblick über den erreichten Stand in Bezug auf die Einhaltung von Sicherheitsbestimmungen und auf notwendige Informationen zur Benutzeraktivität. So können Sie privilegierte Benutzer hinsichtlich der Einhaltung der definierten Rahmenbedingungen und der Sicherheitsrichtlinien überwachen.

Professionelle Module zur Definition von Richtlinien und Berichten für die Erstellung kundenspezifischer Compliancemodule

Die Anpassung Ihrer Berichtsanforderungen an den speziellen Bedarf Ihrer internen Prüfungen oder Complianceanforderungen kann ein langer, aufwendiger Prozess sein. Tivoli Compliance Insight Manager enthält ein Werkzeug für maßgefertigte Berichte, mit dessen Hilfe Sie auch sehr speziellen Berichtsanforderungen gerecht werden können. Die erstellten Berichte können mit Hilfe der automatisierten Berichtsverteilungsfunktion bedarfsgerecht verteilt und so in Prüfungsprozesse oder andere Workflows des Unternehmens integriert werden.

Datenerfassung mit automatisierter, unternehmensweiter Logdatenanalyse

In den meisten Unternehmen werden an tausenden von Stellen Ereignislogs generiert, die alle gesammelt und aufbewahrt werden müssen. Durch automatisierte, zentralisierte Erfassung der Logdateien kann dieser Prozess effizienter gestaltet werden. Mit Hilfe von Tivoli Compliance Insight Manager können Sie Logdaten für Prüfzwecke im gesamten Unternehmen sicher und zuverlässig erfassen, speichern, analysieren und abrufen.

Eine skalierbare Komponente zur Erfassung von Logdaten ermöglicht die zuverlässige und verifizierbare Erfassung systemspezifischer Logdaten von praktisch jeder Plattform aus. Während mit vielen Lösungen nur Systemprotokolle (Syslogs) und SNMP-Protokolle (Simple Network Management Protocol) erfasst werden können, ermöglicht Tivoli Compliance Insight Manager mit einer eigenen Logmanagementebene die Erfassung von Sicherheitslogs nahezu jedes Typs. Dazu gehören:

- *Betriebssystemebene, z.B. IBM System z, IBM System i, IBM AIX, Sun Solaris, HP-UX, Microsoft® Windows® und Linux®.*
- *Auditlogs aus Anwendungen in Form einer Datei oder einer Datenbanktabelle.*
- *Datenbankebene, z.B. IBM DB2 on System z sowie UNIX® und Windows, Oracle Database Server, Microsoft SQL Server und Sybase ACE.*
- *Logdaten von Sicherheitskomponenten über Syslogs und SNMP.*
- *Weitere Tivoli-Produkte, z.B. Tivoli Security Operations Manager, Tivoli Identity Manager und Tivoli Access Manager.*

Um Ihnen den Nachweis der Vollständigkeit und Kontinuität Ihres Logerfassungs- und -managementprogramms gegenüber Prüfern und Behörden zu erleichtern, bietet Tivoli Compliance Insight Manager einen Bericht zur Kontinuität der Logdaten.

Darüber hinaus kann Tivoli Compliance Insight Manager mit optimierten Analysewerkzeugen in einem komprimierten, langfristigen Logdepot Abfragen und Untersuchungen bezüglich verdächtiger Ereignisse durchführen. Das Logdepot stellt benutzerfreundliche Suchfunktionen bereit, um die Erkennung potenzieller Sicherheitsverstöße zu vereinfachen.

Einfache Erweiterung um neue Komponenten zur Erfassung und Analyse von Logdaten

Das professionelle Toolkit von Tivoli Compliance Insight Manager ermöglicht die einfache Erweiterung um neue Komponenten zur Erfassung und Analyse von Logdaten. Diese Parser können zur Definition von Indexierungskomponenten verwendet werden, mit deren Hilfe die aus Logdateien im gesamten Unternehmen stammenden Logdaten in Suchoperationen im Depotanalysewerkzeug aufgenommen werden können. Diese Funktionalität ermöglicht die schnelle Durchführung von Abfragen für sämtliche Onlinelogdaten. Damit erhalten Sie schnelle Reaktionen auf Unternehmensereignisse, ohne sich mit unhandlichen, selbst entwickelten Werkzeugen oder hochgradig technischen Abfragesprachen beschäftigen zu müssen. Nach der Identifizierung von Störungen können die ursprünglichen Logdaten abgerufen und mit anderen plattformspezifischen Analysewerkzeugen weiterverarbeitet werden.

Überwachung und Kontrolle der Aktivität privilegierter Benutzer

In den letzten Jahren wurde den von externen Quellen ausgehenden Sicherheitsrisiken immer mehr Beachtung zuteil. Zwar stellen diese Angriffe eine sehr reale Bedrohung für Unternehmen dar, die internen Sicherheitsverstöße durch privilegierte Benutzer bedeuten häufig jedoch ein noch größeres Sicherheitsrisiko. Ob unbeabsichtigt oder nicht, die Auswirkungen reichen von langwierigen Ausfallzeiten über geschäftliche Einbußen bis zu Haftungspflichten.

Tivoli Compliance Insight Manager ermöglicht Ihnen die Überwachung der Aktivität dieser einflussreichen Benutzer. So können Sie feststellen, ob Ihre Richtlinien durchgängig umgesetzt und eingehalten werden – ohne die privilegierten Benutzer in der schnellen und effektiven Erfüllung ihrer Aufgaben zu behindern.

Bei anstehenden Audits erleichtert Ihnen Tivoli Compliance Insight Manager den Nachweis gegenüber den Prüfern, dass Ihr Unternehmen:

- *Regelmäßig die Aktivität der Systemadministratoren und Systembediener protokolliert und prüft.*
- *Sicherheitsverstöße und verdächtige Vorgänge erkennt und analysiert und Gegenmaßnahmen trifft.*
- *Den Zugriff auf sensible Daten protokolliert, darunter den Root-/Administratorzugriff und den Datenbankadministratorzugriff (DBA).*
- *Anwendungs-, Datenbank-, Betriebssystem- und Einheitenprotokolle durchgängig führt und prüft.*

Erweiterung der IBM RACF-Prüffunktionen durch Plug-ins

Tivoli Compliance Insight Manager bietet zusätzliche Großrechner-Plug-ins mit erweiterten Funktionen für die RACF-Prüfung. Dies senkt den finanziellen und personellen Aufwand zur Aufrechterhaltung einer sicheren Umgebung für Ihre geschäftskritischen Ressourcen. Mit Hilfe dieser Plug-ins, die für die komplette Bandbreite an RACF-spezifischen Fragen der Sicherheit und Konformität entwickelt wurden, können Unternehmen:

- *Großrechnerereignisse schnell analysieren und entsprechende Berichte erstellen.*
- *Mit einer umfangreichen Statusprüfung Sicherheitsrisiken automatisch erkennen.*
- *Standardisierte und angepasste Berichte im XML-Format erstellen, um sie in Datenbanken und Berichtswerkzeugen weiterzuverwenden.*
- *Unbefugte Anmeldeversuche, Sicherheitsrichtlinien verletzendes Benutzerverhalten sowie Risiken für die Kernsysteme schnell erkennen.*
- *RACF-Befehle auf Übereinstimmung mit den Richtlinien und Verfahren Ihres Unternehmens überprüfen und bei Nichtübereinstimmung korrigieren bzw. blockieren.*

Integration mit SIEM-, Identitätsmanagement- und Zugriffssteuerungslösungen

Tivoli Compliance Insight Manager ergänzt Tivoli Security Operations Manager und unterstützt Unternehmen bei der Reaktion auf Störungen und der Einhaltung von Richtlinien. Tivoli Compliance Insight Manager sendet Informationen zu kritischen Ereignissen an Tivoli Security Operations Manager, so dass das für die Sicherheit verantwortliche Personal sofort geeignete Maßnahmen treffen kann. Tivoli Security Operations Manager kann für Tivoli Compliance Insight Manager auch Daten zu Richtlinienverstößen bereitstellen. Zum Beispiel kann Tivoli Security Operations Manager Ausnahmedaten an Tivoli Compliance Insight Manager senden, wenn die Reaktionseiten bei Störungen nicht den Unternehmensrichtlinien entsprechen, so dass das für die Sicherheit verantwortliche Personal diese Ausnahmen untersuchen kann, bevor die Sicherheit oder die Einhaltung der Richtlinien bedroht ist.

Tivoli Compliance Insight Manager kann auch mit Tivoli Identity Manager, IBM Tivoli Access Manager for e-business und IBM Tivoli Access Manager for Operating Systems integriert werden. Diese Integration ermöglicht die Überwachung der administrativen Aktivität auf diesen Servern, um festzustellen, ob die durch die Administratoren für Tivoli Identity Manager und Tivoli Access Manager veranlassten Änderungen oder Vorgänge durch Ihre Richtlinien gedeckt sind. Tivoli Compliance Insight Manager interagiert auch mit den Administratorverzeichnissen von Tivoli Identity Manager und Tivoli Access Manager, so dass die tatsächlichen Benutzernamen der Benutzer mit Verwaltungsaufgaben in Tivoli Compliance Insight Manager-Berichten einbezogen werden können.

Tivoli Compliance Insight Manager auf einen Blick

Mindestanforderungen an Unternehmensserver:

- 4 x Intel® Xeon 3,0 GHz-Prozessor
- 6 GB RAM
- Windows 2000 Advanced Server SP4 oder Windows 2003 Server SP1
- Microsoft Internet Explorer 6.0 oder höher für die Anzeige der HTML-Berichte

Mindestanforderungen an Standardserver:

- 2 x Xeon 3,0 GHz-Prozessor
- 4 GB RAM
- Windows 2000 Advanced Server SP4 oder Windows 2003 Server SP1
- Microsoft Internet Explorer 6.0 oder höher für die Anzeige der HTML-Berichte
- Syslog-NG 1.6.6 oder höher

Die speziellen Anforderungen hängen von dem Logdatenumfang und den Typen der Logdaten ab. Die obigen Angaben stellen die Mindestanforderungen dar.

Weitere Informationen

Auf der Basis über zwanzigjähriger Erfahrung in den Bereichen Sicherheitsprüfung und Compliance-Management bietet Tivoli Compliance Insight Manager eine führende Lösung für die Logdatenanalyse, die Überwachung privilegierter Benutzer und die Erstellung von Audit- und Complianceberichten im gesamten Unternehmen – von den Betriebssystemen und Anwendungen bis hin zu Datenbanken, Großrechnern und Netzeinheiten.

Wenn Sie mehr darüber erfahren möchten, wie Tivoli Compliance Insight Manager Ihr Unternehmen bei der Überwachung der Benutzeraktivität und der Integration der Maßnahmen zur Einhaltung von Richtlinien unterstützen kann, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter:

ibm.com/tivoli

Tivoli-Software von IBM

Tivoli-Software stellt ein umfassendes Paket von Angeboten und Funktionen zur Unterstützung von IBM Service Management zur Verfügung – ein skalierbares, modulares Verfahren, das Ihrem Unternehmen effizientere und effektivere Services bereitstellt. Tivoli erfüllt die Ansprüche von Unternehmen jeder Größe und ermöglicht es Ihnen, durch Integration und Automatisierung von Prozessen, Arbeitsabläufen und Aufgaben hervorragende Services für die Unterstützung Ihrer Geschäftsziele bereitzustellen. Die sichere, auf offenen Standards basierende Service-Management-Plattform Tivoli wird ergänzt durch proaktive Lösungen für operatives Management mit durchgängiger Transparenz und Kontrolle. Sie wird außerdem gestützt durch den hervorragenden IBM Kundendienst, die IBM Unterstützungsfunktion und ein aktives Geschäftsumfeld von IBM Business Partnern. Des weiteren können Tivoli-Kunden und -Geschäftspartner gegenseitig ihre bewährten Verfahren nutzen, indem sie an unabhängigen IBM Tivoli-Benutzergruppen auf der ganzen Welt teilnehmen. Besuchen Sie:

www.tivoli-ug.org

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®

TID10355-DEDE-00