Facilitare i controlli di sicurezza e monitorare gli utenti privilegiati grazie a un dashboard affidabile di conformità della sicurezza

Tivoli software

IBM Tivoli Compliance Insight Manager

Considerazioni principali

- Automatizzare il reporting delle revisioni attraverso un dashboard aziendale di conformità e una distribuzione flessibile dei report
- Creare moduli personalizzati di conformità mediante motori avanzati di definizione di report e policy
- Soddisfare le necessità di audit convertendo i dati di log di verifica nativi acquisiti in una forma facile da comprendere
- Raccogliere, conservare, esaminare e recuperare i log con efficienza grazie alla gestione automatizzata dei log
- Facilitare l'aggiunta di nuovi strumenti di raccolta e analisi dei log grazie a un toolkit avanzato
- Eseguire attività di monitoraggio e verifica degli utenti privilegiati (PUMA, "Privileged-User Monitoring and Audit") su database, applicazioni, server e mainframe
- Integrabile con IBM Tivoli Identity Manager, IBM Tivoli Access Manager e IBM Tivoli Security Operations Manager per contribuire a ottimizzare la conformità e la risposta agli incidenti.

Molte aziende si trovano nella necessità di gestire quantità ingenti di dati di log che devono essere conservati per le revisioni delle autorità competenti. Innanzi tutto, i log devono essere raccolti in modo affidabile e verificabile da punti d'origine dispersi per tutta la struttura aziendale, e queste operazioni devono avvenire in modo continuo e sostenibile. Una volta acquisiti miliardi di voci di log, occorre un modo rapido ed efficiente per dare loro un significato.

Raccogliere e organizzare queste informazioni può richiedere una notevole quantità di tempo ed esperienza. Molte organizzazioni – le cui risorse sono già sfruttate al massimo – non hanno semplicemente né il tempo né il personale. Per questo c'è IBM Tivoli Compliance Insight Manager. Tivoli Compliance Insight Manager, una soluzione automatizzata per il monitoraggio, l'analisi e il reporting dell'attività degli utenti in azienda, può fornire, in modo continuo e non intrusivo, sicurezza e prove documentali che i propri dati e sistemi vengano gestiti secondo le policy aziendali.

Comprendere rapidamente le attività degli utenti grazie a un dashboard completo

Tivoli Compliance Insight Manager offre un dashboard di conformità della sicurezza facile da usare, che riassume miliardi di file di log in una sola grafica di riepilogo. Tramite questo dashboard, è possibile avere una rapida panoramica del proprio profilo di conformità della sicurezza, inquadrare le attività degli utenti e gli eventi di sicurezza rispetto a standard di utilizzo accettabili e monitorare gli eventi di sicurezza e gli utenti privilegiati.

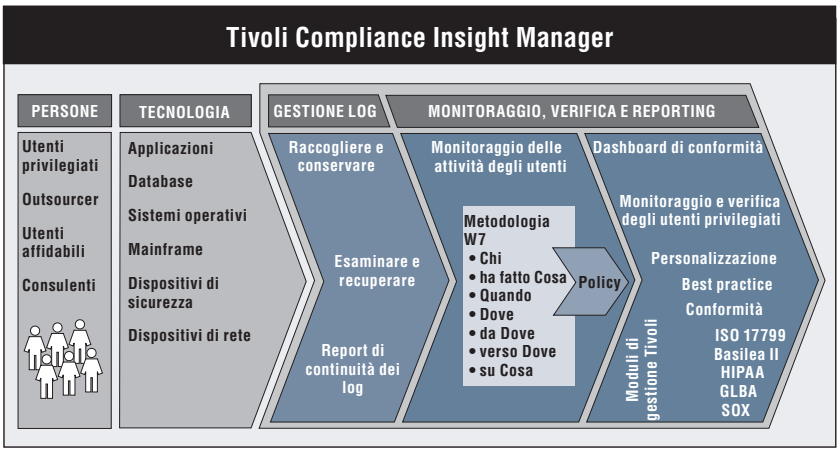
Grazie alla sua metodologia W7, in corso di brevetto, Tivoli Compliance Insight Manager converte i dati nativi dei log in una forma facile da comprendere. L'efficace combinazione tra la metodologia W7 e il dashboard grafico aiuta a verificare con facilità le "sette W": chi (Who) ha fatto cosa (What), quando (When), dove (Where), da dove (Where from), verso dove (Where to) e su cosa (on What).

Con queste informazioni a portata di mano, è possibile:

- *Esaminare in profondità il comportamento degli utenti, l'attività dei sistemi e le informazioni di sicurezza su tutti i tipi di piattaforma.*
- *Confrontare le voci dei log con la policy di base per contribuire a individuare e ridurre al minimo i problemi di sicurezza.*
- *Mettere a disposizione report in risposta alle richieste di dimostrazioni da parte degli ispettori e alle necessità di indagini dei responsabili della sicurezza, senza doversi rivolgere a costosi esperti in materia.*
- *Rispondere rapidamente agli incidenti grazie alla possibilità di impostare azioni e avvisi relativi all'attività degli utenti privilegiati, consentendo allo stesso tempo agli amministratori di fare il loro lavoro.*

Comunicare efficacemente le informazioni relative a revisioni e conformità e automatizzare la distribuzione dei report

Acquisire e convertire i dati dei log in modo continuativo e completo può ridurre notevolmente il carico di lavoro dovuto all'osservanza dei requisiti di conformità. Tivoli Compliance Insight Manager offre ben più di questo, consentendo alle organizzazioni di produrre istantaneamente report orientati agli utenti e ai dati, e offrendo soluzioni di reporting personalizzato e condizionale per rispondere a specifiche necessità di reporting.

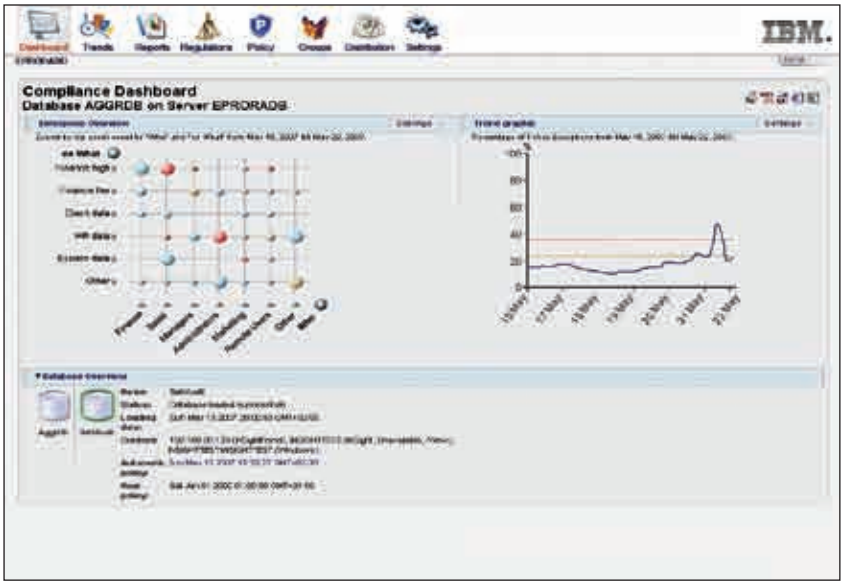


Tivoli Compliance Insight Manager acquisisce informazioni di sicurezza relative a persone e tecnologia per il reporting di conformità e verifica.

Inoltre, Tivoli Compliance Insight Manager offre più di 100 report (best practice, report per revisioni e gestione conformità) per aiutare a soddisfare i requisiti di reporting aziendali e di revisioni esterne. I diversi modelli – completi di policy personalizzabili di uso accettabile per definire i gruppi e le policy W7 – consentono un avvio rapido dei processi di monitoraggio e reporting. Il generatore di policy automatizzato aiuta a stabilire le policy di base che serviranno come fondamenta per le analisi future; inoltre è possibile personalizzare i confronti per adattarli meglio alle policy di sicurezza specifiche della propria organizzazione.

Grazie al dashboard completo per la verifica e conformità, i responsabili della sicurezza possono visualizzare immediatamente lo stato di conformità dell'organizzazione, il che consente loro di individuare con precisione le aree critiche e le potenziali violazioni che richiedano analisi e correzione immediate.

Inoltre, la funzionalità di distribuzione automatizzata dei report consente di definire con facilità gli elenchi di distribuzione dei report. Questi report possono essere inviati ai responsabili aziendali per ulteriori verifiche o per gli eventuali altri interventi richiesti dai processi di business interni.



Il dashboard di Tivoli Compliance Insight Manager consente di avere una rapida panoramica del proprio profilo di conformità della sicurezza, inquadrare le attività degli utenti e monitorare gli eventi di sicurezza rispetto agli standard di utilizzo accettabile e alle policy di sicurezza.

Creare moduli di conformità personalizzati mediante motori avanzati di definizione di report e policy

La definizione di requisiti di reporting su misura per le necessità specifiche e dettagliate dei propri requisiti interni di verifica o conformità può essere un processo lungo e noioso. Lo strumento di reporting personalizzato di Tivoli Compliance Insight Manager consente di adattarsi perfettamente alle necessità di reporting specifiche della propria organizzazione. I report creati, inoltre, possono essere distribuiti mediante la funzione di distribuzione automatizzata dei report in modo da consentire l'integrazione con i processi di verifica o con altre parti dei processi di business.

Acquisire dati con un'analisi immediata dei log dell'azienda

Molte organizzazioni hanno migliaia di punti d'accesso distribuiti per tutta l'azienda che generano log degli eventi, e tutti questi log devono essere acquisiti e conservati. Automatizzare e centralizzare la raccolta dei file di log può contribuire a rendere più efficiente il processo, risparmiando così tempo e denaro. Tivoli Compliance Insight Manager aiuta a raccogliere, conservare, analizzare e recuperare i log dell'intera azienda, con sicurezza e affidabilità, per poterli utilizzare in attività di conformità e analisi.

Un sistema scalabile di raccolta di log contribuisce ad assicurare una raccolta affidabile e verificabile dei log nativi praticamente da qualsiasi piattaforma. Laddove molte soluzioni raccolgono solo i syslog e i log SNMP (Simple Network Management Protocol), il livello di gestione log di Tivoli Compliance Insight Manager può acquisire quasi ogni tipo di log di sicurezza, tra cui:

- *Log a livello di sistema operativo, tra cui IBM System z, IBM System i, IBM AIX, Sun Solaris, HP-UX, Microsoft® Windows® e Linux®.*
- *Tracce di verifica delle applicazioni, scritte su file o su una tabella di database.*
- *Log a livello database, tra cui IBM DB2 su System z oppure su UNIX® e Windows, Oracle Database Server, Microsoft SQL Server e Sybase ACE.*
- *Log dei dispositivi di sicurezza, mediante syslog e SNMP.*
- *Altri prodotti Tivoli, come Tivoli Security Operations Manager, Tivoli Identity Manager e Tivoli Access Manager.*

Per aiutare a consegnare a ispettori e autorità pubbliche report immediati sulla completezza e continuità del proprio programma di raccolta e gestione dei log, Tivoli Compliance Insight Manager offre il report di continuità dei log.

Inoltre, con i suoi strumenti di analisi ottimizzati, Tivoli Compliance Insight Manager può analizzare e ricercare evenienze sospette all'interno di un archivio di log compresso di lungo periodo. L'archivio di log offre funzionalità di ricerca facili da utilizzare per contribuire a individuare i potenziali incidenti di sicurezza.

Facilitare l'aggiunta di nuovi strumenti di raccolta e analisi dei log

Il toolkit avanzato di Tivoli Compliance Insight Manager semplifica l'aggiunta di nuovi strumenti di raccolta e analisi dei log. Questi strumenti di analisi consentono di definire strumenti di indicizzazione che consentono ai dati di log – raccolti dai file di log dell'intera azienda – di essere inclusi nelle ricerche dello strumento di analisi dell'archivio dei log. Questa funzionalità consente di eseguire con rapidità query che spaziano su tutti i dati di log on-line. Pertanto, è possibile ottenere risposte veloci agli incidenti in azienda senza dover ricorrere a ingombranti strumenti sviluppati internamente dall'azienda o linguaggi di query altamente tecnici. Una volta individuati gli incidenti, è possibile recuperare i dati di log originari e utilizzarli con strumenti di indagine o strumenti di analisi specifici per una data piattaforma.

Monitorare e controllare le attività degli utenti privilegiati

Negli ultimi anni, i rischi di sicurezza dovuti a fonti esterne hanno ricevuto un'attenzione significativa dai media. Se da una parte questi attacchi di alto profilo sono certamente una minaccia reale per le organizzazioni, gli incidenti di sicurezza interni a opera di utenti privilegiati spesso sono minacce ancora maggiori. Colposo o doloso che sia, le conseguenze possono variare: dalle interruzioni prolungate dei servizi, alla perdita di clienti, alle responsabilità legali.

Tivoli Compliance Insight Manager consente di monitorare le attività di questi utenti che hanno notevole libertà di azione, in modo da poter verificare che le policy vengano sempre rispettate – senza limitare la possibilità, da parte degli utenti privilegiati, di fare il loro lavoro in modo rapido ed efficiente.

Quando si avvicinano le verifiche periodiche, Tivoli Compliance Insight Manager può aiutare a dimostrare agli ispettori che la propria organizzazione:

- *Registra e analizza le attività degli amministratori e operatori di sistema con regolarità.*
- *Analizza e indaga sugli incidenti di sicurezza e sulle attività sospette, ed esegue interventi di correzione.*
- *Registra l'accesso ai dati sensibili, compresi gli accessi root/amministratore e DBA (amministratore database) database.*
- *Conserva e analizza regolarmente log di applicazioni, database, sistemi operativi e dispositivi.*

Migliorare le capacità di verifica IBM RACF grazie ai plug-in

Tivoli Compliance Insight Manager offre plug-in opzionali per mainframe con funzionalità avanzate per la verifica RACF, contribuendo a ridurre i costi e le competenze necessari a mantenere un ambiente sicuro per le risorse critiche dell'azienda. Progettati per rispondere all'intera gamma di problemi di conformità e sicurezza specifici per RACF, questi plug-in consentono alle organizzazioni di:

- *Analizzare e redigere report sui mainframe rapidamente.*
- *Rilevare automaticamente i punti esposti della sicurezza grazie a verifiche di stato intensive.*
- *Stilare report standard e personalizzati che possono essere generati in formato XML per essere utilizzati con database e strumenti di reporting.*
- *Determinare rapidamente gli accessi e tentativi di accesso non autorizzati, i comportamenti degli utenti che violano le policy di sicurezza e i momenti in cui i sistemi centrali sono a rischio.*
- *Verificare i comandi RACF confrontandoli con le policy e le procedure della propria azienda, e bloccare o correggere quelli che non corrispondono.*

Integrarsi con le soluzioni di gestione delle identità, di controllo di accesso e SIEM

Tivoli Compliance Insight Manager si integra con Tivoli Security Operations Manager per aiutare le organizzazioni a migliorare la risposta agli incidenti e la conformità alle policy. Inviando informazioni riguardo gli eventi critici da Tivoli Compliance Insight Manager a Tivoli Security Operations Manager, il personale operativo di sicurezza può intervenire immediatamente. Tivoli Security Operations Manager inoltre può fornire dati di violazione delle policy a Tivoli Compliance Insight Manager. Per esempio, Tivoli Security Operations Manager può inviare dati relativi alle eccezioni a Tivoli Compliance Insight Manager nel caso in cui i tempi di risposta agli incidenti eccedano quanto indicato nella policy aziendale, consentendo così al personale di sicurezza di indagare su queste eccezioni prima che possano porre problemi alle misure di conformità o di sicurezza.

Inoltre, Tivoli Compliance Insight Manager è integrabile con Tivoli Identity Manager, IBM Tivoli Access Manager for e-business e IBM Tivoli Access Manager for Operating Systems. Questa integrazione consente di monitorare le attività amministrative su questi server per determinare se le modifiche e le attività degli amministratori di Tivoli Identity Manager e Tivoli Access Manager rientrano nelle policy o nelle direttive di utilizzo accettabili. Tivoli Compliance Insight Manager, inoltre, è integrabile con le directory di amministrazione del software Tivoli Identity Manager e Tivoli Access Manager, pertanto i nomi utente effettivi degli utenti amministratori sono inclusi nei report di Tivoli Compliance Insight Manager.

Panoramica di Tivoli Compliance Insight Manager

Requisiti minimi del server, versione enterprise:

- 4 processori Intel® Xeon 3.0GHz
- 6GB di RAM
- Windows 2000 Advanced Server con SP4 o Windows 2003 Server con SP1
- Microsoft Internet Explorer 6.0 o superiore per visualizzare i report HTML

Requisiti minimi del server, versione standard:

- 2 processori Xeon 3.0GHz
- 4GB di RAM
- Windows 2000 Advanced Server con SP4 o Windows 2003 Server con SP1
- Microsoft Internet Explorer 6.0 o superiore per visualizzare i report HTML
- Syslog-NG 1.6.6 o successivo

I requisiti specifici dipenderanno dai volumi di log e dai tipi di dati di log. Le voci sopra riportate rappresentano i requisiti minimi.

Ulteriori informazioni

Basato su un'esperienza più che ventennale nella gestione della conformità e delle verifiche di sicurezza, Tivoli Compliance Insight Manager offre la migliore soluzione sul mercato per l'analisi dei log, il monitoraggio degli utenti privilegiati e il reporting per conformità e verifiche sull'intera azienda – da sistemi operativi e applicazioni a database, mainframe e dispositivi di rete.

Per ulteriori informazioni su come Tivoli Compliance Insight Manager può aiutare la vostra organizzazione a monitorare le attività degli utenti e integrare le attività di conformità, contattate il vostro rappresentante IBM o Business Partner IBM, oppure visitate il sito:

ibm.com/it/tivoli

Informazioni sul software Tivoli di IBM

Il software Tivoli mette a disposizione un insieme di prodotti e di funzionalità a supporto di IBM Service Management, un approccio scalabile e modulare per fornire servizi più efficienti ed efficaci alle vostre attività. Contribuendo a rispondere alle esigenze di aziende di ogni dimensione, il software Tivoli consente di fornire servizi di qualità a supporto dei vostri obiettivi di business, attraverso l'integrazione e l'automazione di processi, flussi di lavoro e attività. La piattaforma Tivoli per la gestione dei servizi, all'avanguardia in fatto di sicurezza e basata su standard aperti, viene integrata da soluzioni di gestione operativa in grado di offrire visibilità e controllo a tutto campo. Inoltre è supportata da servizi IBM riconosciuti a livello mondiale, dal Supporto IBM e da tutta l'organizzazione dei Business Partner IBM. I clienti e business partner Tivoli possono inoltre trarre vantaggio dalla condivisione delle best practice, partecipando ai Gruppi di Utenti IBM Tivoli, gestiti autonomamente – visitate il sito:

www.tivoli-ug.org

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate
Milano

La home page di IBM Italia si trova all'indirizzo:
ibm.com/it

Disclaimer: Il cliente ha la responsabilità di assicurare la conformità ai requisiti legali. È esclusiva responsabilità del cliente ottenere la consulenza di un legale per l'identificazione e l'interpretazione di ogni legge rilevante e ogni requisito normativo che possano interessare le proprie attività di affari e ogni azione che potrebbe dover intraprendere per essere conformi con tali leggi. IBM non fornisce alcun consiglio legale né garantisce che i suoi prodotti o servizi assicurino che l'utente si trovi in conformità con qualsiasi legge o normativa.

Stampato negli Stati Uniti d'America
06-07

TAKE BACK CONTROL WITH Tivoli

TID10355-ITIT-00