IBM PowerSC

Progettato per la sicurezza e la conformità delle aziende negli ambienti virtualizzati e cloud

Caratteristiche principali

- Semplificazione della gestione e della misurazione di sicurezza e conformità
- Panoramica rapida della conformità della sicurezza di un intero data center grazie a un'interfaccia utente centralizzata
- Riduzione dei tempi e dei costi di amministrazione relativi alle attività di conformità ai requisiti normativi
- Migliori funzioni di audit per i sistemi virtualizzati a fronte di una riduzione dei tempi e delle capacità necessari per la preparazione
- Miglioramento nell'individuazione dell'esposizione ai rischi negli ambienti virtualizzati.

Il controllo della sicurezza e la conformità sono alcuni dei componenti chiave necessari per difendere i data center virtualizzati e l'infrastruttura cloud da minacce in evoluzione. Riuscire a garantire la conformità dei sistemi IT agli standard di sicurezza del settore e la sicurezza dei sistemi può essere molto impegnativo e richiedere notevoli investimenti in termini di costi e risorse umane, in particolar modo negli attuali ambienti IT cloud/virtualizzati. IBM® PowerSC offre una soluzione di sicurezza e conformità ottimizzata per gli ambienti virtualizzati e cloud sui server Power Systems in esecuzione su PowerVM.

PowerSC è un'offerta integrata, che garantisce elevati livelli di sicurezza e conformità grazie alle caratteristiche dello stack di IBM Power Systems Software, a partire da hypervisor e firmware fino al livello di virtualizzazione del sistema operativo (SO), incluso il traffico di rete tra i livelli.

PowerSC riduce i costi, semplifica l'amministrazione, accelera la preparazione delle verifiche di conformità e riduce i rischi aumentando la visibilità delle minacce alla sicurezza.

Impostazioni di sistema automatiche per una sicurezza e una conformità ottimali

Le caratteristiche del settore in cui operano impongono a molti clienti IBM Power System la stretta aderenza a precisi standard di conformità. Per riuscire a garantire il rispetto di questi standard di conformità è necessario impostare regole di sicurezza sui sistemi in modo uniforme. Purtroppo lo studio delle regole e l'applicazione di uno specifico standard è sono attività impegnative, che richiedono molto tempo e sono spesso soggette ad errori. Gli standard di conformità sono di solito documenti

lunghi e complessi, composti da centinaia di regole, difficili da trasformare in impostazioni appropriate per il sistema operativo. Inoltre, poiché gli standard spesso riguardano diverse aree del sistema operativo e del software di virtualizzazione, possono richiedere l'utilizzo di diverse interfacce amministrative per configurare il sistema in modo appropriato.

Le funzioni automatiche di conformità di PowerSC offrono profili integrati ntegrati certificati per assicurare la conformità rispetto a standard quali PCI (Payment Card Industry Data Security Standard) v3, HIPAA (Health Insurance Portability and Accountability Act Privacy and Security Rules) per il settore sanitario, NERC (North American Electric Reliability Corporation) per utility come il settore energetico, DoD STIG (US Department of Defence Security Technical Implementation Guide per UNIX) per i nostri clienti dell'amministrazione Federale, oltre al supporto per SOX-COBIT (best practice Sarbanes - Oxley previste per lo standard Control Objectives for Information and related Technology). PowerSC offre anche un profilo di automazione della sicurezza, per automatizzare la configurazione della sicurezza ottimale per i server di database. Inoltre, prevede livelli OOTB (out of the box) per livelli di scurezza classificati Low, Medium e High.

Il meccanismo integrato PSCxpert (una versione avanzata di AIXpert) permette di attivare le impostazioni delle policy di sicurezza e i controlli di conformità. Si tratta di strumenti che si sono sempre dimostrati eccellenti per la gestione della conformità. Tuttavia, per gestire i profili è sempre stato necessario eseguire l'accesso e lanciare i comandi individualmente sui singoli sistemi. La nuova interfaccia utente (UI) centralizzata di automatizzazione della conformità, introdotta nella versione 1.1.5 di PowerSC, ha semplificato notevolmente la gestione della conformità (cfr. sezione: "Nuova interfaccia centralizzata per conformità e sicurezza")

Monitoraggio e generazione di avvisi in caso di modifiche ininterrotti

La funzione RTC (Real Time Compliance) permette di monitorare un elenco di file e invia una notifica nel caso si verificasse una violazione della conformità o venisse rilevata una modifica a uno dei file sottoposti a controllo. In genere, vengono eseguiti controlli di conformità ad intervalli regolari. Così, se il sistema dovesse versare in uno stato di non conformità, non sarebbe possibile accorgersene fino all'avvio del controllo successivo. La funzione RTC invece annulla questo gap temporale, dal momento che la notifica viene inviata nel momento stesso in cui si verifica una qualsiasi violazione della policy prevista per il server. Nell'istante esatto in cui una modifica apportata dovesse determinare il venir meno della conformità è possibile prevedere l'invio di una notifica agli amministratori o ai responsabili della sicurezza tramite SMS (Short Message Service) o email. È inoltre possibile inviare messaggi SNMP (Simple Network Management Protocol) e Syslog al server di controllo, integrando la relativa funzione nel sistema di monitoraggio IT. Prodotti quali IBM QRadar sono in grado di ricevere questi avvisi e integrarli nell'infrastruttura esistente.

La funzione RTC di PowerSC prevede due opzioni di monitoraggio:

1. *Monitoraggio dei contenuti* che verifica l'eventuale modifica del contenuto di un file

2. *Monitoraggio degli attributi* che verifica l'eventuale mondifica dei permessi

Nuova interfaccia centralizzata per conformità e sicurezza

La nuova interfaccia centralizzata per conformità e sicurezza – introdotta con la versione 1.1.5 di PowerSC e poi ampliamente estesa nella versione 1.1.6 – ha semplificato notevolmente la gestione della conformità, con una sensibile riduzione di costi, tempi ed errori umani.

- **Automazione della conformità**
  Esamina e gestisce la conformità di sicurezza di tutti gli endpoint AIX gestiti da PowerSC nell'ambiente Power richiedendo un minimo impegno di ricerca e sfruttando una posizione centralizzata. Consente di controllare e applicare profili PowerSC, scegliendo tra profili personalizzati e integrati, su più endpoint contemporaneamente. Inoltre, permette di organizzare e raggruppare gli enpoint PowerSC, applicando filtri personalizzati.
- **Integrazione RTC / TE**
  Funzionalità avanzate di rilevamento e prevenzione dell'intrusione di malware, grazie alla configurazione centralizzata e alla funzionalità di controllo di File Integrity Monitoring (PowerSC RTC e AIX TE).
- **Integrazione PowerVC**
  Consente di proteggere i cloud fin dalle primissime operazioni. Il processo è stato semiautomatizzato e consente di connettere i nuovi endpoint in fase di distribuzione con PowerVC come nuovi endpoint gestiti all'interno della nuova interfaccia utente di PowerSC UI.
- **Dashboard di sicurezza e conformità**
  Offre una vista riassuntiva di tutti i principali componenti di protezione e tracciamento AIX.
- **Reporting to support audits**
  PowerSC 1.1.6 viene fornito con cinque report OOTB che consentono di preparare i controlli for / pass. È possibile creare file formattati in formato html o csv, che possono essere inviati automaticamente ad orari prestabiliti via email.
- **Miglioramenti dell'editor di profilo**
  Questa funzionalità nella versione 1.1.5 aveva limitate capacità di creazione di profili personalizzati; il nuovo editor di profilo incluso nella versione 1.1.6 consente ai clienti di integrare fra loro regole di profili diversi così da creare un profilo personalizzato. Inoltre, consente di modificare i parametri delle singole regole interne ai profili personalizzati.
- **Integrazione Northbound (QRadar)**
  Nella versione 1.1.6 il lavoro sull'integrazione ha utilizzato strumenti di sicurezza di livello più elevato attraverso informazioni syslog, per consentirne l'utilizzo da parte di QRadar.
- **Miglioramenti del processo UNDO**
  Il processo di ANNULLAMENTO di un profilo è piuttosto complesso. Nella versione PowerSC 1.1.6 il comportamento del processo UNDO è stato migliorato per il profilo PCIv3. Il comportamento del processo UNDO degli altri profili verrà migliorato nelle successive versioni.
- **Scalabilità dell'interfaccia utente per la conformità**
  PowerSC è in grado di supportare 500 endpoint con l'interfaccia server della versione 1.1.5. Con la versione 1.1.6, il numero è stato raddoppiato a 1.000 endpoint.

Nota: gli altri componenti di PowerSC (TNC, Trusted Boot, Trusted Firewall, Trusted Logging) continuano ad esistere nelle loro versioni native (riga di comando) all'interno dell'attuale versione;

La versione della nuova interfaccia centralizzata di conformità e sicurezza è supportata solo nei sistemi AIX

Conformare le macchine virtuali alle policy di sicurezza del sito

La gestione delle Macchine Virtuali (VM) su più sistemi presenta difficoltà operative superiori a quelle dei sistemi fisici tradizionali. Ad esempio, le VM possono essere sospese o disattivate o perfino spostate su altri server durante il processo di applicazione di una patch. Il trasferimento di una VM può, ad esempio, aprire una finestra di vulnerabilità dovuta a un livello di patch diverso da quello richiesto sul sistema fisico di destinazione.

TNC (Trusted Network Connect) e Patch Management in PowerSC rilevano le VM AIX che non soddisfano le policy delle patch aziendali stabiliti per un data center virtualizzato. Qualora venga rilevata una VM non conforme, viene generato un avviso. TNC e Patch Management analizzano i dati SUMA (Service Update Manager Assistant) e NIM (Network Installation Manager) per controllare ciascuna VM durante il processo di attivazione della rete.

TNC e Patch Management monitorano anche il sistema IBM Electronic Customer Care e generano avvisi quando vengono rilevati nuovi aggiornamenti o patch di sicurezza che incidono sul funzionamento dei sistemi AIX. Inoltre, è possibile attivare un servizio di SMS per ricevere avvisi sui dispositivi mobili.

Nell'ultima versione TNC e Patch Management monitorano anche il software open-source fornito nell'ambito della base AIX per pacchetti che sono stati scaricati dalla toolbox di AIX o altri siti Web di download per AIX Open Source Packages.

Maggiore visibilità e solidità dell'infrastruttura virtuale

PowerSC mette a disposizione una serie di funzioni che garantiscono l'affidabilità delle VM, tra cui "Trusted Boot", l'implementazione virtuale di TPM (Trusted Platform Module) di Trusted Computing Group. La funzione Trusted Boot di PowerSC include la funzionalità virtuale TPM per le VM AIX che operano con l'hypervisor PowerVM su Power Systems.

La funzionalità TPM misura il processo di avvio del sistema per ciascuna VM e, in combinazione con la tecnologia AIX Trusted Execution, garantisce la sicurezza e l'affidabilità dell'immagine di avvio sul disco, dell'intero sistema operativo e dei livelli applicativi. Ciascuna VM dispone di un TPM virtuale separato che contiene dati di misurazione unici utilizzati per convalidare l'affidabilità delle VM. Questa funzionalità è disponibile su tutti gli IBM Power Systems con tecnologia POWER8 o su sistemi provvisti di firmware eFW7.4 o superiore.

PowerSC offre anche OpenPTS, un monitor che consente agli amministratori di monitorare e attestare l'affidabilità delle VM AIX.

Rafforzare i percorsi di audit negli ambienti virtuali

Trusted Logging in PowerSC centralizza i registri di sistema AIX di tutte le VM presenti su un server, consentendo di conservare i registri su un'unica istanza di PowerVM VIOS (Virtual I/O Server). Questa VM di sicurezza VIOS protegge tutti i dati dei registri ricevuti da ciascuna VM AIX. Nessun amministratore delle VM AIX può rimuovere o alterare i registri di sistema presenti sul server di sicurezza VIOS.

Grazie alla centralizzazione dei registri e dell'amministrazione tramite Trusted Logging, il backup, l'archiviazione e la verifica dei registri di sistema risultano notevolmente semplificati per l'amministratore della sicurezza.

Controllo e applicazione della conformità per le reti virtuali

La funzionalità Trusted Firewall di PowerSC mette a disposizione un firewall virtuale per il filtro e il controllo di rete nell'ambito della virtualizzazione del server locale. Il firewall virtuale migliora le prestazioni e riduce il consumo di risorse di rete mediante un traffico di rete locale diretto e sicuro da VM a VM. Trusted Firewall consente di controllare il traffico e offre indicazioni sul traffico da aggiungere al firewall. Questo advisor può generare i comandi appropriati per aggiungere i segmenti di rete VM a Trusted Firewall.

Le funzionalità di sicurezza e conformità di PowerSC prevedono i seguenti componenti:

Compliance Automation con profili preconfigurati per diversi standard di settore	• L'automazione offerta da PowerSC prevede diversi profili integrati certificati per assicurare la conformità rispetto a standard quali PCIv3, HIPAA, NERC, DoD STIG, SOX-COBIT.
Real Time Compliance (RTC) con funzionalità di reportistica	• Semplifica la gestione, attraverso l'automazione del controllo e l'invio di avvisi automatici che permettono agli amministratori di avere una visibilità continua del sistema e una percezione immediata dei casi in cui una modifica dovesse violare una delle regole che la policy preconfigurata identifica come violazione della conformità per i sistemi AIX.
Trusted Network Connect (TNC) e **Patch Management**	• Riconosce automaticamente il sistema AIX di avvio, ripristino o spostamento grazie alla mobilità live nell'ambiente virtuale e verifica il livello previsto per le patch di sicurezza e installazione, con eventuale invio di avvisi in caso di rilascio di patch che interessano i sistemi.
Trusted Boot	• Misura immagine di avvio, SO e applicazioni e attesta il relativo livello di affidabilità e controllo di alterazione involontaria o intenzionale tramite la tecnologia vTPM (virtual Trusted Platform Module).
Trusted Logging	• I log AIX vengono archiviati in modo centralizzato e in tempo reale nel server virtuale di I/O (Virtual input/output Server). Questa funzione garantisce la sicurezza dell'attività di logging oltre che la comodità di gestione e backup ed elimina la necessità di eseguire agenti di analisi dei log nel SO. In questo modo viene preservata la catena di fiducia relativa ai log di audit e di sistema.
Trusted Firewall	• Trusted Firewall assicura che tutte le VM abbiano l'opportuno livello di isolamento in rete. Consente di risparmiare tempo e risorse grazie all'indirizzamento diretto verso specifiche LAN virtuali (VLAN). Le prestazioni risultano ulteriormente migliorate anche dai servizi firewall di rete integrati nel server, che escludono la necessità di un firewall esterno per le VM relativamente al traffico VM sullo stesso CEC.

Ulteriori informazioni

Per maggiori informazioni su IBM PowerSC, contattare il proprio responsabile commerciale o Business Partner (BP) IBM di fiducia o visitare i seguenti siti Web:
ibm.com/systems/power/software/security/index.html

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

Il sito IBM è disponibile all'indirizzo **ibm.com/it**

Si prega di riciclare

PowerSC

POD03063-ITIT-09