Novell Identity and Security Solutions

www.novell.com

Sentinel Log Manager for Small and Medium Business

La proposta di Novell per aiutare le organizzazioni IT alla conformità al Provvedimento del Garante per la Protezione dei dati personali del 27 Novembre 2008

White Paper

Novell.

Sommario

Il Provvedimento

Il 27 Novembre 2008 il Garante per la Protezione dei Dati Personali ha emesso il provvedimento *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.*

Gli "amministratori di sistema" sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione.

Questo il motivo per cui Garante ha deciso di richiamare l'attenzione di enti, amministrazioni, società private sulla figura professionale dell' amministratore di sistema e ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici.

Le ispezioni effettuate in questi anni dall'Autorità hanno permesso di mettere in luce in diversi casi una scarsa consapevolezza da parte di organizzazioni grandi e piccole del ruolo svolto dagli amministratori di sistema. Alcuni gravi casi verificatisi negli ultimi anni hanno evidenziato una preoccupante sottovalutazione dei rischi che possono derivare quando l'attività di questi esperti sia svolta senza il necessario controllo.

Le misure e le cautele dovranno essere messe in atto entro il 15 Dicembre 2009 da parte di tutte le aziende private e da tutti i soggetti pubblici, compresi gli uffici giudiziari, le forze di polizia, i servizi di sicurezza. Sono da considerarsi non compresi invece i trattamenti di dati, sia in ambito pubblico che privato, effettuati esclusivamente a fini amministrativo contabile, che pongono minori rischi per gli interessati.

Gli impatti sull'IT

Buona parte delle misure che le aziende dovranno adottare sono di carattere procedurale ed organizzativo come, ad esempio, il fatto che "*L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato – Art 4.1"* oppure che *"Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza – Art 4.2"*, ma il Provvedimento indica anche alcune misure con un diretto impatto sui sistemi IT, in particolare l'Art. 4.5 che riporta testualmente *"Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema".*

L'Autorità Garante per la Protezione dei Dati Personali fa quindi appello alle organizzazioni a dotarsi di opportuni strumenti in grado di rilevare l'attività di "Autenticazione" da parte degli amministratori sui Sistemi da loro stessi amministrati.

Novell Sentinel Log Manager – La proposta ad alto valore

La recente normativa del Garante Privacy sugli amministratori di sistema ha introdotto la necessita' di uno strumento che sia in grado di:

- Registrare gli accessi degli utenti classificati “Amministratori di Sistema”
- Garantirne la completezza ed inalterabilità
- Mantenere le registrazioni per almeno 6 mesi

Novell Italia, che conosce il mercato delle piccole e medie aziende Italiane, ha preparato **Novell Sentinel Log Manager for Small and Medium Business,** la soluzione ad un costo contenuto ed alto valore che aiuta le aziende ad ottenere i requisiti di conformità alle richieste del Garante e qualora future esigenze di monitoraggio della sicurezza informatica o possibili nuove e più stringenti normative lo dovessero imporre, è estendibile in termini di funzionalità e quindi pronto per essere adeguato ai continui cambiamenti.

Si può quindi installare Novell Sentinel Log Manager for SMB in configurazioni minima al fine di ottenere la reportistica necessaria per soddisfare il Provvedimento del Garante Privacy, oppure utilizzarlo per ottenere la globalità delle informazioni provenienti da Sistemi, Applicazioni, Host, Network Device, Database ecc. per avere una completa visibilità di quanto è accaduto sul Sistema Informatico

Novell Sentinel Log Manager for SMB gestisce fino a 500 EPS (Eventi Per Secondo) con una tolleranza di 120 sforamenti di picco all'anno. Qualora il vostro IT produca un maggior numero di Eventi al secondo, Novell Sentinel Log Manager for SMB continua a registrare gli eventi regolarmente, segnalandolo all'amministratore.

Oltre tale soglia si può fare l'upgrade alla versione 2.500 o 7.500 EPS.

Novell Sentinel Log Manager for Small and Medium Business è destinato ad aziende pubbliche o private con meno di 1.000 dipendenti.

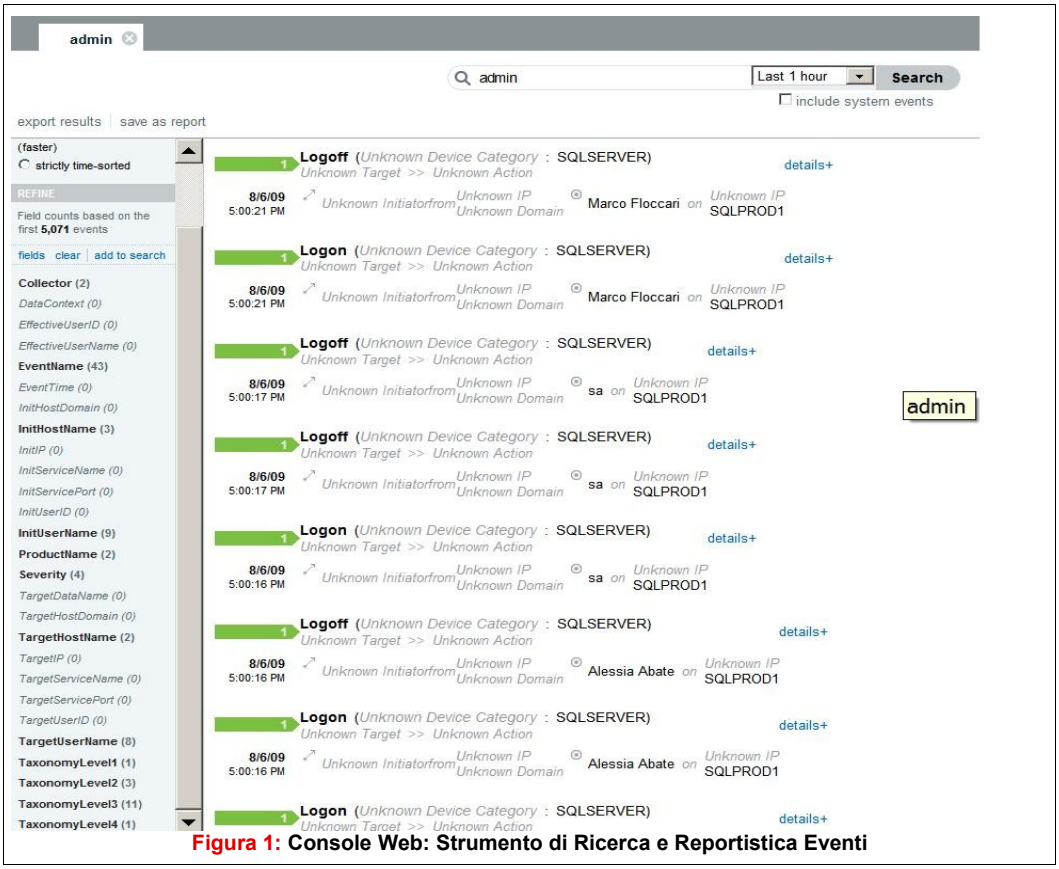

Figura 1: Console Web: Strumento di Ricerca e Reportistica Eventi

Un software di Log Management Sicuro, semplice oggi e potente domani

Novell Sentinel Log Manager for SMB appartiene alla famiglia dei software di “Log management”; questi tools tipicamente hanno un supporto minimale per i diversi formati di log e si appoggiano su protocolli di comunicazione non-sicuri. Inoltre si appoggiano su sistemi di storage proprietari e costosi e spesso mancano di un percorso evolutivo verso ciò che è il reale obiettivo di chi vuole raggiungere una visibilità globale ed automatizzata della Security: il SIEM (Security Information and Event Management).

Novell Sentinel Log Manager for SMB è invece tutto questo in un'unica soluzione: facile da installare e da utilizzare; garantisce conformità al Provvedimento del garante Privacy oggi, ma può diventare un potentissimo strumento di SIEM domani.

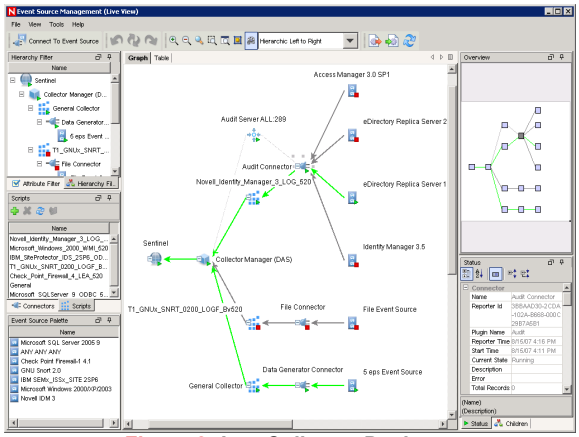

Figura 2: Log Collector Designer

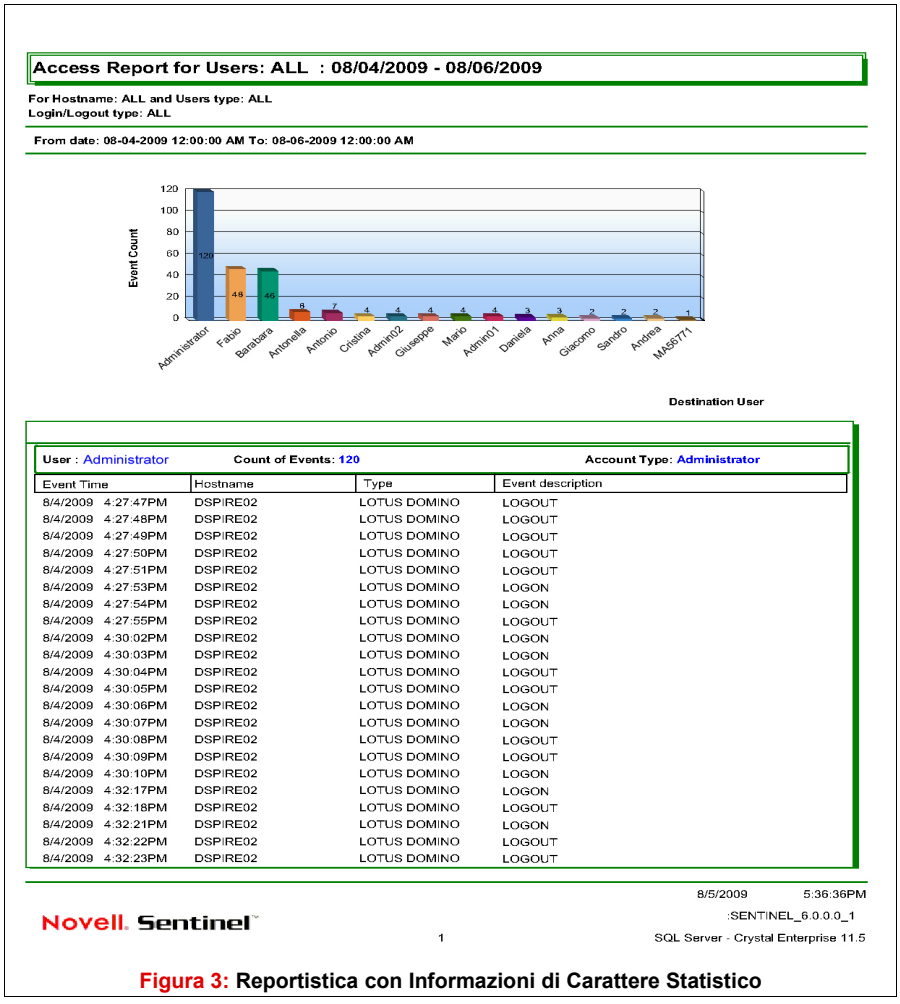

Figura 3: Reportistica con Informazioni di Carattere Statistico

Colleziona i dati in modo flessibile ma sicuro

Se la maggior parte dei software della categoria dei Log Management dipendono pesantemente dal syslog su User Datagram Protocol, Novell Sentinel Log Manager for Small and Medium Business ha già out-of-the-box il supporto nativo sia per syslog che per il collezionamento di altri protocolli. Oltre che su UDP supporta anche syslog su protocolli sicuri ed affidabili come TCP e TLS. Novell Sentinel Log Manager for SMB rileva in automatico I diversi tipi di sorgenti di informazioni (come PIX*, Linux * e Solaris*) ed ha un collettore universale syslog per eventi syslog che non è in grado di riconoscere.

Diversamente dalle soluzioni dei suoi competitors, Novell Sentinel Log Manager for SMB, può collezionare e gestire dati da sorgenti di log in aggiunta al syslog.

Novell Sentinel Log Manager for SMB si basa sul consolidato prodotto Novell Sentinel ed il proprio framework di raccolta dati che offre una vasta gamma di collettori per Sistemi Operativi, Database, Firewalls, Routers, Intrusion Detection / Intrusion Prevention Systems, Antivirus, Mainframe, Enterprise Application (SAP, Siebel) ed oltre.

Questi collettori, come dice il nome, collettano (o “collezionano”), normalizzano, filtrano ed arricchiscono di informazioni I dati di log per facilitare analisi future, ricerche o fatti avvenuti in passato.

Si ottengono i Reports con un Click

E' vero che molti dei tools di log management includono dei modelli di reports, ma questi sono tipicamente poco utili senza un preventivo ed intenso lavoro di personalizzazione; Novell Sentinel Log Manager for SMB semplifica egregiamente la generazione dei reports con il proprio sistema di indicizzazione dei dati ed un semplicissimo strumento di generazione di report da parte anche di utenti inesperti.

Utilizzando questo trumento di reportistica basato sulle API open Source LUCENE, si può facilmente immettere i criteri di ricerca su cui si desidera il report e Novell Sentinel Log Manager for SMB crea immediatamente i reports che sono più comunemente richiesti dagli auditors ai fini di comprovare la conformità alle normative quali il Provvedimento al Garante Privacy per gli Amministratori di Sistema.

Con un solo click questi sono già ottenibili in formato presentabile a un Auditor.

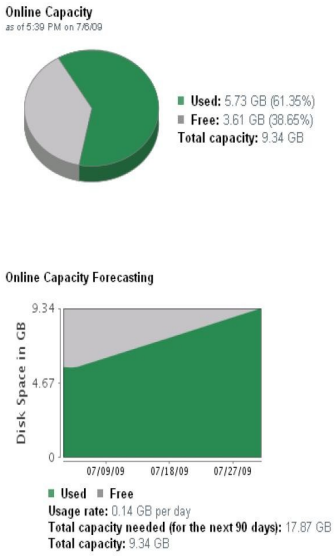

Figura 4: **Gestione dello Storage**

Query e Reports sia su dati On-Line che sui dati Archiviati

Via via che i dati di log diventano più datati, si tende normalmente ad archiviarli su storage per lunga durata. Quando però si necessita di avere un report su dati che sono parte on-line e parte archiviati, prima è necessario riportare on-line tutti i dati archiviati per poi lanciare la query: niente di più lungo ed inutile. Novell Sentinel Log Manager for SMB consente invece di effettuare query e reports simultaneamente su entrambi i data stores, accorciando significativemente i tempi.

Event Monitoring, Interfaccia facile ed intuitiva

Novell Sentinel Log Manager for SMB si basa sulla tecnologia Web 2.0 che rende l'uso intuitivo e particolarmente facile per l'utente. è tramite questa interfaccia che si può facilmente rilevare le tendenze di utilizzo di certi sistemi, applicazioni oppure identificare problemi. Si possono inoltre schedulare reports, regole di ritenzione dei dati di log, configurare le policies di filtraggio o azioni come ad esempio l'invio di e-mails, mandare dei traps SNMP, scrivere files oppure trasmettere le informazioni a Sentinel perchè prenda eventuali contromisure in real-time all'accadere di eventi considerati potenzialmente pericolosi.

Un Data Storage Flessibile ed Ottimizzato

Molti produttori di software di Log Management utilizzano sistemi proprietari di storage. Oltre al fatto di rendere più costosa l'architettura, questo approccio crea dipendenza nell'utilizzo dei tool di

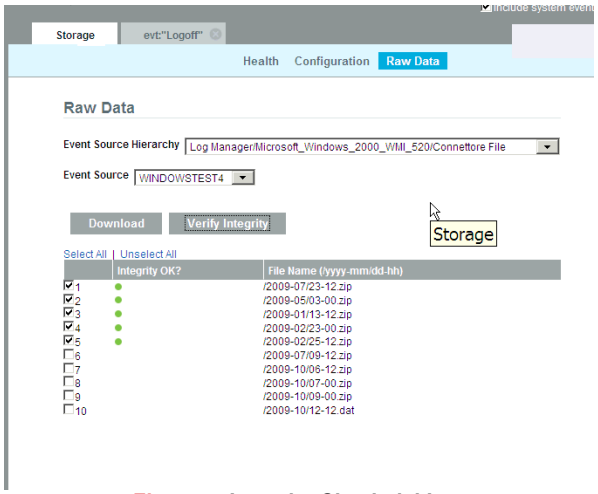

Figura 5: **Integrity Check dei Log**

query e reportistica. Inoltre non si è in grado di fare analisi sui dati senza fare operazioni di backup e restore e ciò rende difficile dimostrare con certezza assoluta che tali dati non siano stati alterati. Novell Sentinel Log Manager for SMB invece sorpassa questi ostacoli registrando i dati collezionati su sistemi di storage standard ed aggiungendo la "signature" dei dati per assicurare le "caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste" (Così come richiesto dal Garante).

Novell Sentinel Log Manager for SMB inoltre ottimizza lo spazio occupato sullo storage comprimendo automaticamente i dati con un coefficiente di 10:1. Si connette inoltre facilmente alla vostra SAN o NAS per espandere la necessità di spazio quando occorre.

Il primo passo verso il SIEM e lo IAM

Si realizza così il primo passo verso una gestione omnicomprensiva della Security come solo un vero SIEM (Security Information and Event Management) consente. Novell Sentinel Log Manager for SMB permette già da subito di rendersi conformi con la normativa Provvedimento del Garante sugli amministratori di Sistema, ma grazie alla sua modularità è possibile aggiungervi Novell Sentinel che permette la rilevazioni di incidenti, anomalie o violazioni in real-time. Passo successivo potrà essere l'Identity and Access Management introducendo le funzioni di User Provisioning, Gestione di Autenticazioni, Accessi, Cambi Passwords, Strong Authentication ed i molti altri temi di Security che Novell fornisce già integrate ed in grado di dimostrare conformità a qualunque normativa relativa alla Security – legislativa o non – presente e futura.

Elementi Chiave e Differenzianti di Novell Sentinel Log Manager for SMB

- *Condivide larga parte dell'architettura e del codice sorgente con il consolidato Novell Sentinel utilizzato nelle piu' grando Telco, Banche o ambienti militari;*
- *Rilevamento automatico dei sorgenti di log*
- *Supporta il collezionamento di messaggi di log da sorgenti sconosciute;*
- *Supporta il collezionamento dei dati ad un elevato coefficiente di Eventi per Secondo;*
- *Ricerche su dati On-Line ed archiviati simultaneamente;*
- *Conversione di ricerche in reports riutilizzabili e molti formati di reportistica pre-confezionati*
- *Permette di fare query con perfezionamenti e rifiniture approfondite tramite criteri di ricerca con Hyperlink;*
- *E' dotato Out-of-the-box di numerosi reports soprattutto a fini forensi*
- *E' basato su tecnologia Web 2.0 che aggiornano automaticamente i dati a video quando qualcosa si aggiunge o cambia;*
- *Comprime i dati automaticamente per massimizzare le capacità degli storage;*
- *Usa la signature delle righe di log per garantire la integrità ed inalterabilità;*
- *Memorizza le informazioni su SAN/NAS standard, no hardware proprietario;*
- *Permette facilmente di personalizzare le regole di data rentention;*
- *Interfaccia AJAX base, facile ed "user-friendly";*
- *Installazione facile e rapida;*
- *Possibile primo passo per passaggi successivi a SIEM e/o IAM;*