

Novell Sentinel Log Manager

Bezpieczne, łatwe i efektywne zarządzanie rejestrami zdarzeń

Novell.

Zgodność z przepisami – prosto, inteligentnie i ekonomicznie

Większość firm i instytucji stoi obecnie wobec konieczności gromadzenia, przechowywania i zarządzania rejestrami zdarzeń (logami) pochodzącymi ze wszystkich systemów informatycznych i aplikacji w celu skutecznego ograniczania ryzyka i zapewniania zgodności z wymogami przepisów. Rozwiązania do zarządzania rejestrami zdarzeń zaspokajają potrzeby w zakresie gromadzenia i przechowywania danych w sposób zapewniający niedrogie zbieranie, składowanie i zarządzanie dużymi ilościami danych o zdarzeniach. Zebrane dane o zdarzeniach mogą być przechowywane i przeszukiwane w celu udostępnienia przejrzystej historii zdarzeń, wspomaganie wewnętrznych dochodzeń i procesów sądowych oraz tworzenia raportów niezbędnych dla audytów lub wymaganych przez przepisy.

Rozwijając się i dążąc do zwiększenia dynamiki i konkurencyjności, firmy sięgają po nowatorskie rozwiązania techniczne, zapewniające efektywną eksploatację infrastruktury informatycznej i sprawną współpracę z partnerami, klientami i pracownikami. Wdrażając nowe technologie, firmy napotykają na szereg trudności, począwszy od problemów natury technicznej, takich jak kwestie zgodności interoperacyjnej, bezpieczeństwa lub zgodności z wymogami przepisów, po problemy biznesowe związane z kosztami, wiarygodnością marki czy zaufaniem klientów. Przy całej złożoności środowisk informatycznych, zadania związane z zapewnianiem bezpieczeństwa i zgodności z wymogami przepisów dodatkowo komplikuje obecność coraz liczniejszych i coraz bardziej wyrafinowanych zagrożeń zewnętrznych i wewnętrznych.

Rozwiązania do zarządzania rejestrami zdarzeń stały się niewątpliwym fundamentem zarządzania bezpieczeństwem i zapewniania zgodności z wymogami przepisów. Wraz z pojawieniem się modelu rozszerzonych korporacji (obejmujących swym zasięgiem nie tylko pracowników) i wzrostem złożoności funkcjonowania aplikacji i systemów, efektywne monitorowanie i zarządzanie milionami zdarzeń informatycznych stało się dla wielu firm poważnym obciążeniem i źródłem ogromnych kosztów. Państwowe i branżowe przepisy, takie jak PCI-DSS, HIPAA, SOX i GLBA, narzucają zwiększone wymagania w stosunku do zarządzania informacjami o zdarzeniach, a także politykami dostępu uprzywilejowanych użytkowników oraz przechowywania danych. W związku z tym firmy coraz częściej poszukują rozwiązań umożliwiających efektywne zarządzanie rejestrami zdarzeń, które zapewnią im większe bezpieczeństwo, pozwolą ograniczyć ryzyko i ułatwią spełnianie wymagań przepisów bez konieczności ponoszenia nadmiernych kosztów.

Novell Sentinel Log Manager to rozwiązanie do zarządzania rejestrami zdarzeń, odznaczające się wyjątkową elastycznością i skalowalnością. Ma ono postać wirtualnego urządzenia, obejmującego system SUSE Linux Enterprise Server 11 i oprogramowanie Sentinel Log Manager z usługą aktualizacji. Sentinel Log Manager wykorzystuje doskonałe technologie Novella i wbudowany w Novell Sentinel mechanizm integracji, będący efektem doświadczenia w dziedzinie zarządzania informacjami o bezpieczeństwie i zdarzeniach (*SIEM, Security Information & Event Management*) oraz zarządzania tożsamością. Dzięki temu umożliwia gromadzenie i zarządzanie informacjami o zdarzeniach w sposób ukierunkowany na zagwarantowanie zgodności z wymogami przepisów, ograniczanie ryzyka i zapewnianie bezpieczeństwa.

Novell Sentinel Log Manager umożliwia:

- Aktywne ograniczanie ryzyka i *uproszczenie zapewniania zgodności z przepisami*
- *Zmniejszenie kosztów wdrożenia i zarządzania*
- *Wykorzystanie istniejących zasobów sprzętowych*
- *Stworzenie skalowalnego i elastycznego fundamentu dla zgodności z przepisami i bezpieczeństwa.*

Możliwości i zalety

Zaawansowane, elastyczne mechanizmy gromadzenia danych o zdarzeniach

Novell Sentinel Log Manager udostępnia najbardziej elastyczne i skalowalne mechanizmy gromadzenia danych o zdarzeniach. Dzięki wykorzystaniu technologii Novell Sentinel, Novell Sentinel Log Manager wyróżnia się elastycznością i zaawansowanymi możliwościami gromadzenia danych, w tym wbudowaną obsługą formatu syslog i innych protokołów. Czyni go to doskonałym rozwiązaniem do gromadzenia danych z różnorodnych systemów i aplikacji, takich jak systemy wykrywania włamań, firewalle, systemy operacyjne, routery, serwery witryn internetowych, bazy danych, przełączniki sieciowe, komputery mainframe, oprogramowanie antywirusowe i wiele innych. Novell Sentinel Log Manager może wykorzystywać do zbierania danych wiele bezpiecznych protokołów komunikacyjnych, zapewniających spójność danych, a także automatycznie wykrywać źródła rejestrów zdarzeń. Zapewnia również możliwość zbierania i przetwarzania w ograniczonym zakresie nierozpoznanych komunikatów. Przy wszystkich tych zaletach wyróżnia się wysoką szybkością gromadzenia informacji o zdarzeniach (*EPS, events-per-second*).

Znakomite możliwości wyszukiwania i raportowania

Novell Sentinel Log Manager umożliwia regionalną agregację danych, a także łatwe wyszukiwanie i raportowanie zdarzeń w różnorodnych aplikacjach i urządzeniach. Uruchamiany jednym kliknięciem mechanizm raportowania wykorzystuje gotowe szablony raportów, pozwalając w prosty sposób przekształcić wyniki wyszukiwania w bogate, przejrzyste raporty, w tym opisujące stan systemów Windows, stan zgodności z wymogami przepisów na wysokim poziomie, niepomyślnie logowania, modyfikacje kont itd. Zapytania i wyszukiwania obejmują dane bieżące i archiwalne bez konieczności pobierania danych z archiwum w celu ich przeszukania. Istnieje możliwość szybkiego przeszukiwania danych strukturyzowanych i niestrukturyzowanych, dostępna jest także funkcja wyszukiwania rozproszonego, umożliwiającą administratorom przeszukiwanie wielu menedżerów rejestrów zdarzeń z poziomu jednej centralnej konsoli.

Wyniki wyszukiwania Sentinel Log Manager zawierają hiperłącza, umożliwiające dalsze przeszukiwanie wyników i doprecyzowanie kryteriów wyszukiwania. Dostępne są gotowe mechanizmy raportowania i indeksowanego wyszukiwania *ad hoc*, w tym śledczego wyszukiwania *ad hoc*.

Co ważne, oparte na Web 2.0 narzędzia wyszukiwania zawarte w Novell Sentinel Log Manager natychmiast automatycznie odświeżają wyniki, jeśli wyszukiwanie przyniosło nowe rezultaty.

Kontrola dostępu oparta na rolach

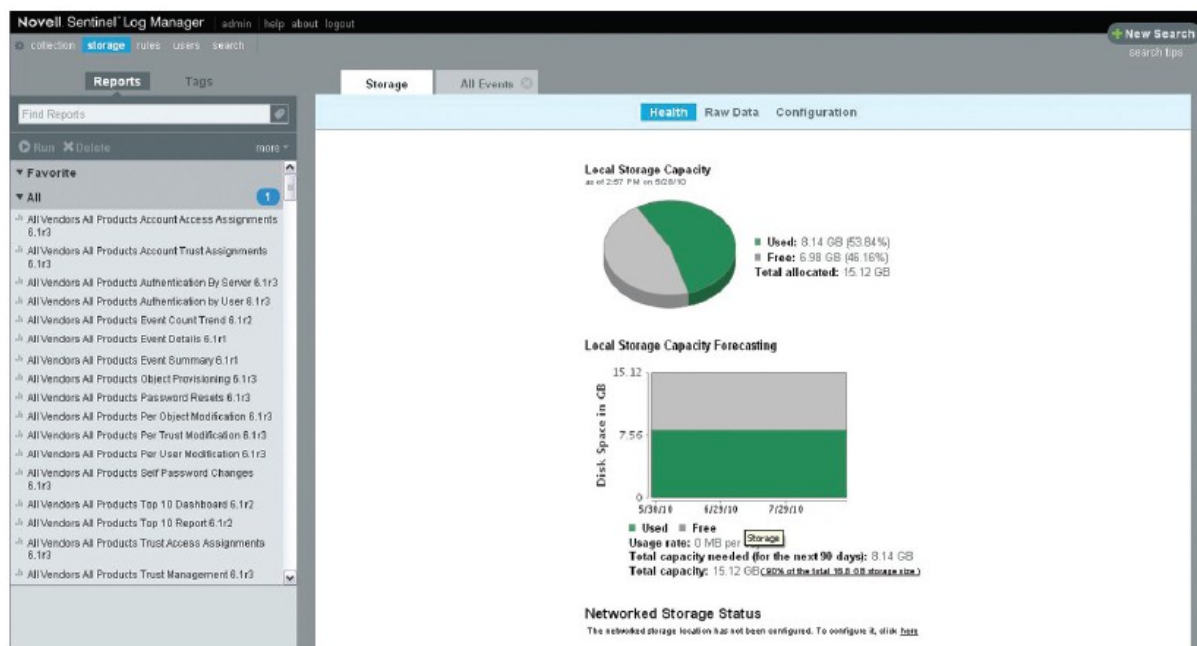
Sentinel Log Manager obsługuje również prawa dostępu dla grup użytkowników, zapewniając precyzyjną kontrolę dostępu do danych, raportów i wyszukiwania. Może oznaczać dane pochodzące z rozmaitych zasobów

(poszczególnych punktów końcowych, serwerów, kolektorów, konektorów i zdarzeń) w celu określenia, kto ma prawo dostępu do informacji powiązanej z owymi zasobami. Udostępnia również globalne reguły filtrowania, oznaczające wszystkie zdarzenia o określonej charakterystyce (np. adresie IP), ograniczając dostęp do tych zdarzeń tylko do określonych użytkowników lub grup. Taka precyzyjna kontrola dostępu pozwala ograniczyć zbędny dostęp do danych, zapewniając jednocześnie użytkownikom dostęp do informacji koniecznych do wykonywania pracy.

Bezpieczne i ekonomiczne przechowywanie danych

Novell Sentinel Log Manager umożliwia wykorzystanie istniejącego standardowego sprzętu i pamięci masowych, zapewniając przy tym składowanie informacji o zdarzeniach o dużej intensywności zmian oraz długotrwałe przechowywanie danych. Wykorzystuje automatyczną kompresję danych w stosunku 10:1, zwiększającą efektywną pojemność nośników, a także obsługuje sygnatury gromadzonych rejestrów, gwarantując spójność danych.

Rozwiązanie wykorzystuje typowe pamięci masowe online, a także systemy SAN/NAS, rozszerzające przestrzeń składowania danych archiwalnych. Umożliwia to zmniejszenie kosztów składowania rejestrów zdarzeń, pozwalając wykorzystywać w tym celu posiadany sprzęt. Definiowalne polityki składowania umożliwiają administratorom określanie, jak długo zgromadzone dane mają być przechowywane online przed automatycznym przeniesieniem do zasobów archiwalnych, a także jak długo mają pozostać w archiwum, zanim zostaną usunięte.



Rys. 1. Konsola zarządzania pamięciami masowymi

Proste i ekonomiczne możliwości wdrożenia

W celu uproszczenia i obniżenia kosztów wdrożenia, przewidziano możliwość zainstalowania Novell Sentinel Log Manager w sposób tradycyjny, jako oprogramowanie w środowisku SUSE Linux Enterprise Server 11, bądź jako wirtualne urządzenie programowe. Oba te warianty umożliwiają wykorzystanie istniejącego sprzętu

i infrastruktury, dzięki czemu Novell Sentinel Log Manager zapewnia znaczną elastyczność, niewielkie koszty oraz duże możliwości zarządzania, szczególnie w porównaniu do rozwiązań sprzętowych.

Choć rozwiązania w postaci urządzeń sprzętowych mogą się wydawać prostsze do wdrożenia, wymagają one zazwyczaj wykorzystania oddzielnego urządzenia w postaci kolektora bądź parsera danych, a także dedykowanego urządzenia archiwizacyjnego, co w istocie zwiększa ich koszt i złożoność. Urządzenia sprzętowe odznaczają się także mniejszą elastycznością i skalowalnością – zwiększenie potencjału wymaga zakupu nowego sprzętu. W przypadku zarządzania rejestrami zdarzeń, większy koszt urządzeń sprzętowych nie przekłada się na dodatkową wartość, ponieważ nie wykorzystują one zwykle wyspecjalizowanego sprzętu. W przypadku Sentinel Log Manager sprzęt można dopasować do konkretnych potrzeb, ograniczając wydatki na drogą wyposażenie tam, gdzie nie jest ono konieczne.

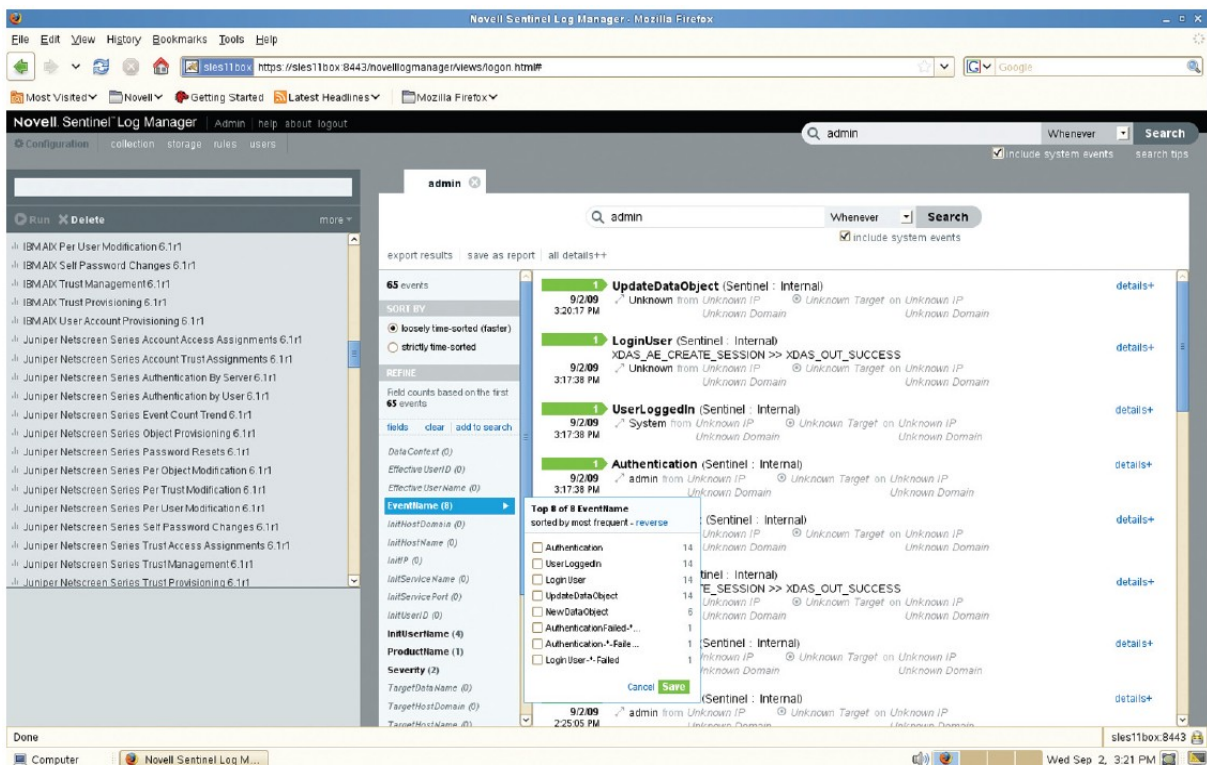
Wdrożenie Novell Sentinel Log Manager w postaci wirtualnego urządzenia programowego obejmuje fabrycznie skonfigurowaną wersję produktu oraz solidnie zabezpieczony system SUSE Linux Enterprise Server 11 w wersji „just-enough-operating-system”, zoptymalizowanej do współpracy z Sentinel Log Manager. Urządzenie programowe dostępne jest w rozmaitych formatach, np. w postaci obrazów maszyn VMware czy XEN lub samoczynnie instalowanego obrazu ISO, które można instalować w środowisku wybranego hipernadzorcy bądź na „czystej” maszynie.

Wirtualne urządzenie Novell Sentinel Log Manager pozwala wykorzystać istniejące zasoby środowisk wirtualnych bez konieczności inwestowania w nowy sprzęt. Oprócz tego wirtualne urządzenie Sentinel Log Manager daje się skalować w miarę wzrostu potrzeb w zakresie zarządzania rejestrami zdarzeń bez konieczności zakupu dodatkowego sprzętu. Wirtualne urządzenie objęte jest również usługą automatycznej aktualizacji zarówno rozwiązania Sentinel Log Manager, jak systemu operacyjnego, dzięki czemu praktycznie nie wymaga pielęgnacji. Podsumowując, wirtualne urządzenie Sentinel Log Manager oznacza prostsze wdrożenie, mniejsze problemy z administrowaniem, niższe całkowite koszty posiadania oraz szybszy zwrot inwestycji, niż w przypadku innych rozwiązań.

Intuicyjny, dynamiczny i łatwy w użyciu interfejs użytkownika

Novell Sentinel Log Manager wykorzystuje opartą na Ajax technologii Web 2.0, obsługującą intuicyjny, łatwy w użyciu i dynamiczny interfejs użytkownika, przejrzyste ukazujący trendy wykorzystania danych i ułatwiający wykrywanie potencjalnych problemów. Pozwala on również konfigurować gromadzenie danych, planować raporty i zarządzać nimi, tworzyć polityki składowania danych, a także konfigurować reguły filtrowania danych i działania, takie jak wysyłanie alarmów pocztą elektroniczną, ustawianie pułapek SNMP, zapisywanie zdarzeń do pliku, a nawet przekazywanie ich do oprogramowania Novell Sentinel w celu natychmiastowego przetworzenia. Interfejs użytkownika udostępnia również funkcje wyszukiwania i raportowania.

Oprócz interfejsu Web 2.0 typu „*thin client*”, Novell Sentinel Log Manager udostępnia również na żądanie interfejs typu „*thick client*” dla bardziej zaawansowanych operacji, takich jak wdrażanie, konfigurowanie i zarządzanie kolektorami danych. Wykorzystując aplikację Java Swing, Sentinel Log Manager pozwala w dowolnej chwili załadować klienta z poziomu dowolnej przeglądarki internetowej i usunąć go z pamięci po zakończeniu sesji. W ten sposób można go wykorzystać bez względu na miejsce pobytu, dysponując jego wszystkimi możliwościami bez konieczności instalowania oprogramowania.



Rys. 2. Interfejs użytkownika w stylu Web 2.0

Element kompletnej implementacji rozwiązania SIEM

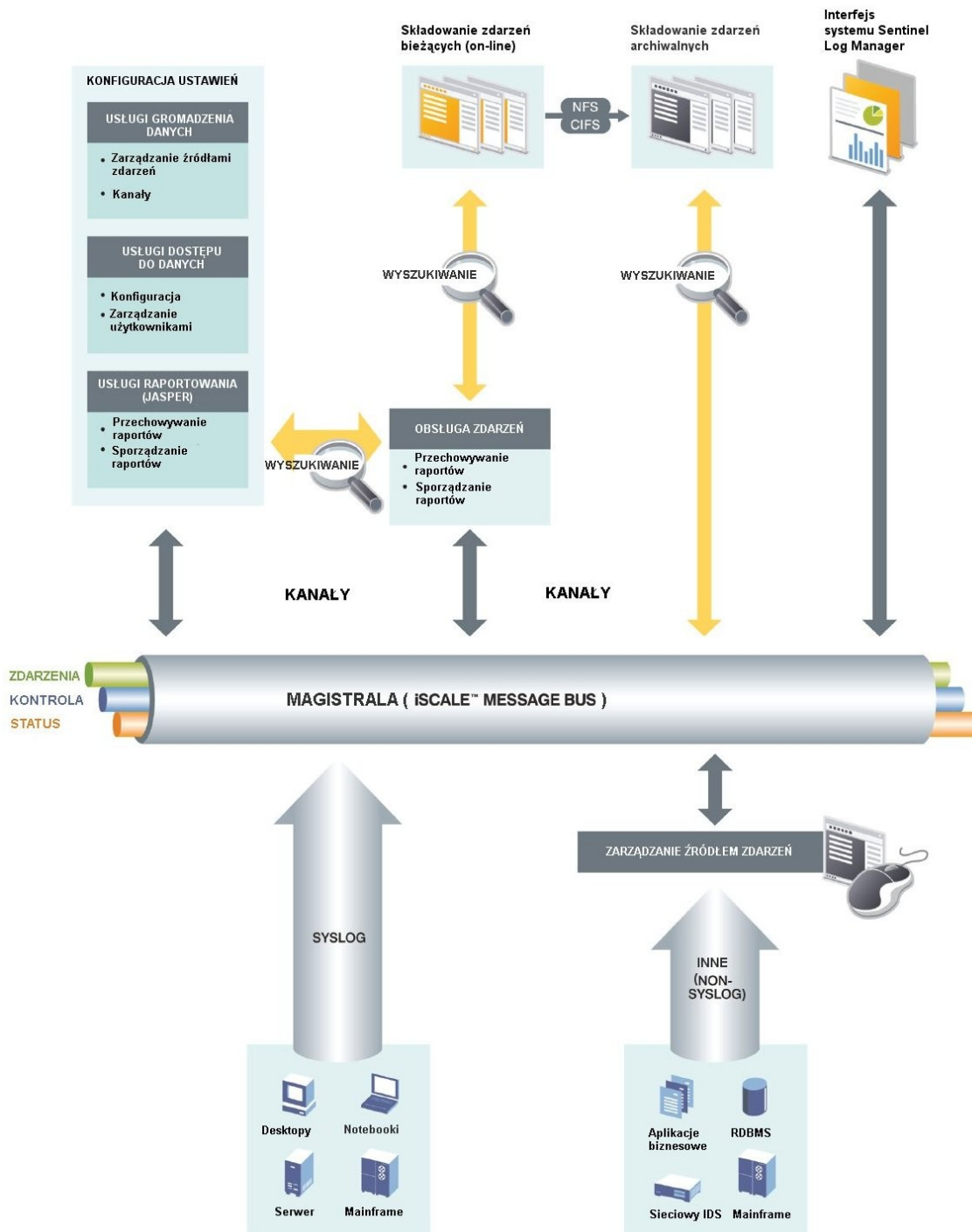
Stanowiąc łatwe i szybkie do wdrożenia rozwiązanie, pozwalające radzić sobie z problemami wynikającymi z wymogami przepisów i potrzebami audytów, Novell Sentinel Log Manager jest również solidnym elementem kompletnej implementacji rozwiązania SIEM (Security Information & Event Management). Gdy już Novell Sentinel Log Manager zbiera dane z urządzeń, może je łatwo przekazywać do rozwiązania Sentinel. Pozwala to wykorzystać inwestycję w zarządzanie rejestrami zdarzeń do zmniejszenia złożoności wdrożenia SIEM. Większość produktów do zarządzania rejestrami zdarzeń nie zapewnia integracji czy też łatwej drogi do pełnej implementacji SIEM. Sentinel Log Manager umożliwia łatwą integrację z mechanizmami monitorowania w czasie rzeczywistym zawartymi w rozwiązaniu Novell Sentinel, a także z zestawem Novell Compliance Management i rozwiązaniami Novella do zarządzania tożsamością i dostępem. Novell Sentinel Log Manager otwiera prostą drogę do kompleksowego rozwiązania problemu bezpieczeństwa z uwzględnieniem tożsamości, pozwalając łatwo rozbudowywać funkcjonalność w miarę zwiększania potrzeb w zakresie bezpieczeństwa i monitorowania zgodności z wymogami przepisów.

Podsumowując, Novell Sentinel Log Manager pozwala:

- Aktywnie ograniczać ryzyko i uprościć działania dla zapewnienia zgodności z przepisami
- Zmniejszyć koszty wdrożenia i zarządzania
- Wykorzystać istniejący sprzęt
- Utworzyć skalowalny, elastyczny fundament zarządzania bezpieczeństwem i zapewniania zgodności z wymogami przepisów

Najważniejsze zalety architektury

Choć Novell Sentinel Log Manager został stworzony w oparciu o technologie gromadzenia danych wbudowane w Novell Sentinel, stanowi jednocześnie elastyczne, niezależne rozwiązanie do zarządzania rejestrami zdarzeń. Ma także możliwość integracji z funkcjami czasu rzeczywistego Novell Sentinel, przekazując mu zbierane informacje o zdarzeniach za pomocą mechanizmu Sentinel Link. Zbudowany w oparciu o skalowalną architekturę, Sentinel Log Manager jest w stanie sprostać potrzebom najbardziej wymagających środowisk. Aby zagwarantować bezpieczeństwo, Sentinel Log Manager przesyła wszystkie komunikaty w postaci zaszyfrowanej.



Rys. 3. Architektura Novell Sentinel Log Manager

Architektura Novell Sentinel Log Manager obejmuje następujące główne usługi i elementy:

- *Magistrala komunikatów*
- *Usługi gromadzenia danych*
- *Usługi dostępu do danych*
- *Sentinel Link*
- *Składowanie zdarzeń bieżących*
- *Składowanie zdarzeń archiwalnych*
- *Pamięć konfiguracji*
- *Usługi zdarzeń*

Magistrala komunikatów

Novell Sentinel Log Manager wykorzystuje tę samą architekturę magistrali komunikatów, co Novell Sentinel. Magistrala komunikatów, oparta na architekturze Sonic Java Message Service (JMS), zapewnia łatwą komunikację między wszystkimi elementami Sentinel Log Manager, a także komunikację z Novell Sentinel i innymi rozwiązaniami zdolnymi do tego rodzaju komunikacji, takimi jak system Novell Identity Manager.

Koncepcja architektury magistrali komunikatów jest kluczowa dla wysokiej skalowalności systemu Novell Sentinel Log Manager. Umożliwia ona rozbudowę poszczególnych elementów rozwiązania (np. odpowiedzialnych za gromadzenie danych) o kolejne urządzenia i uruchamianie ich na wielu rozproszonych serwerach w ramach tego samego systemu, bez konieczności dokupowania licencji baz danych oraz kosztownego sprzętu.

Magistrala komunikatów izoluje poszczególne elementy Novell Sentinel Log Manager, dzięki czemu żadna usługa nie musi czekać, aż inna usługa zakończy działanie. Zapewnia to w porównaniu z konkurencyjnymi rozwiązaniami znacznie szybsze wykonywanie zapytań, raportów i innych operacji. Eliminuje to również obecność w systemie pojedynczych punktów awarii. Cechą zapewniającą wysoką wydajność i skalowalność jest zdolność Sentinel Log Manager do efektywnego wykorzystania systemów wieloprocesorowych.

Magistrala komunikatów umożliwia rozdzielenie obciążeń związanych z poszczególnymi elementami, dzięki czemu różne usługi mogą działać niezależnie na różnych rdzeniach procesorów i nie generują wzajemnych opóźnień.

Usługi gromadzenia danych

Usługi gromadzenia danych mogą działać na tym samym serwerze, co Novell Sentinel Log Manager, lub na innych komputerach, co znakomicie ułatwia tworzenie systemów rozproszonych. Usługi gromadzenia danych zbierają dane o zdarzeniach z różnych rodzajów urządzeń i źródeł, systemów operacyjnych i aplikacji, a następnie rejestrują je w postaci skorelowanej do dalszej analizy.

Podczas gdy większość rozwiązań do zarządzania rejestrami zdarzeń przyjmuje dane w formacie syslog za pośrednictwem UDP, usługi gromadzenia danych Novell Sentinel Log Manager obsługują fabrycznie zarówno syslog, jak i rodzime formaty w innych protokołach. Oprócz UDP, można korzystać z formatu syslog za pośrednictwem bardziej bezpiecznych i niezawodnych protokołów TCP i TLS/SSL, zapewniających

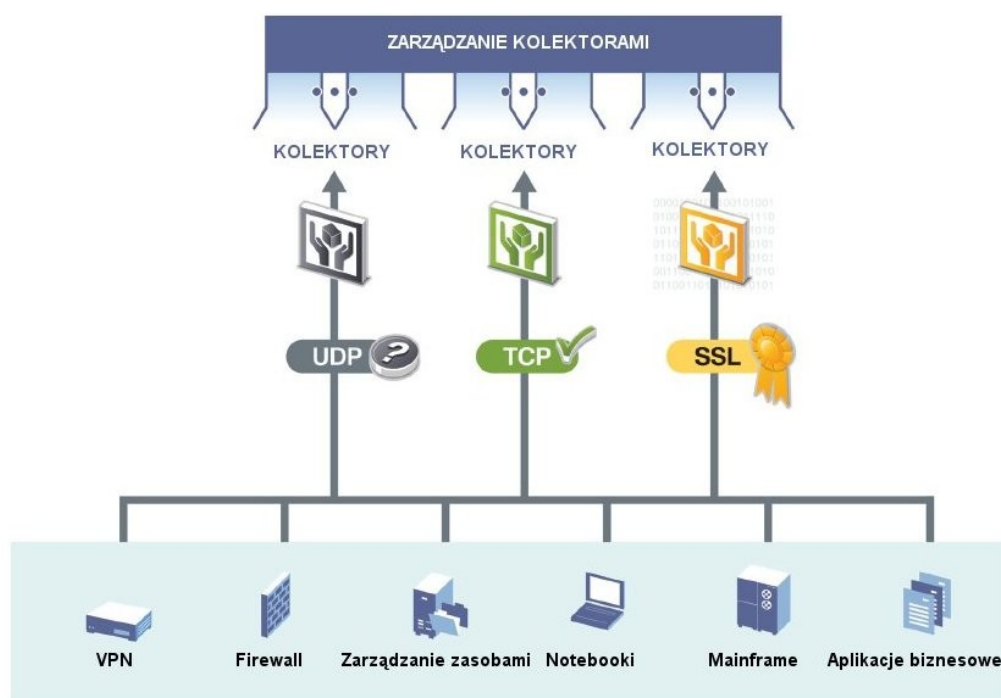
uwierzalnianie oraz obsługę certyfikatów. Novell Sentinel Log Manager umożliwia automatyczne wykrywanie różnych rodzajów źródeł (np. PIX, Linux i Solaris) i jest wyposażony w uniwersalny kolektor dla nierozpoznanych zdarzeń syslog.

Istotną zaletą Novell Sentinel Log Manager w stosunku do konkurencyjnych rozwiązań są szerokie możliwości gromadzenia i zarządzania danymi ze źródeł innych niż syslog. Oprócz standardowej funkcji obsługi syslog, Novell Sentinel Log Manager wyposażony jest również w sprawdzony mechanizm integracji danych Sentinel z bogatym zestawem kolektorów danych z systemów operacyjnych, baz danych, katalogów, firewalli, systemów wykrywania i zapobiegania włamaniom, programów antywirusowych, komputerów typu mainframe, serwerów witryn i aplikacji internetowych i wielu innych źródeł.

Oprócz dostarczanych, gotowych kolektorów, użytkownicy mogą konfigurować, dostosowywać czy też tworzyć własne, odpowiadające konkretnym potrzebom kolektory.

Interpretujące kolektory zbierają dane o zdarzeniach z różnych źródeł i dokonują ich normalizacji do standardowego formatu o wspólnym układzie pól, co ułatwia ich korelowanie i tworzenie raportów. Dokonują również rozbioru danych, wstawiając metatagi, ułatwiające późniejszą analizę, wizualizację i raportowanie zdarzeń, co usprawnia działania na rzecz zapewniania bezpieczeństwa i zgodności z wymogami przepisów. Kolektory automatyzują również proces filtrowania zdarzeń, eliminując nieistotne dane już w punkcie gromadzenia, co zmniejsza obciążenie sieci i przestrzeni dyskowej.

Dzięki elastycznej architekturze, Novell Sentinel Log Manager umożliwia zakup jednej z opcji zapewniającej określoną wydajność dostosowaną do konkretnych, bieżących potrzeb użytkownika. W chwili obecnej dostępne są trzy główne opcje zakupowe. Obejmują one Sentinel Log Manager 500 EPS, 2500 EPS i 7500 EPS, gdzie liczba oznacza liczbę zdarzeń rejestrowanych w ciągu sekundy. Pozwala to wdrożyć rozwiązanie odpowiednie dla danego środowiska, bez ryzyka przeciążenia bądź konieczności sztucznego ograniczania.



Rys. 4. Novell Sentinel Log Manager obsługuje protokoły UDP, TCP i SSL

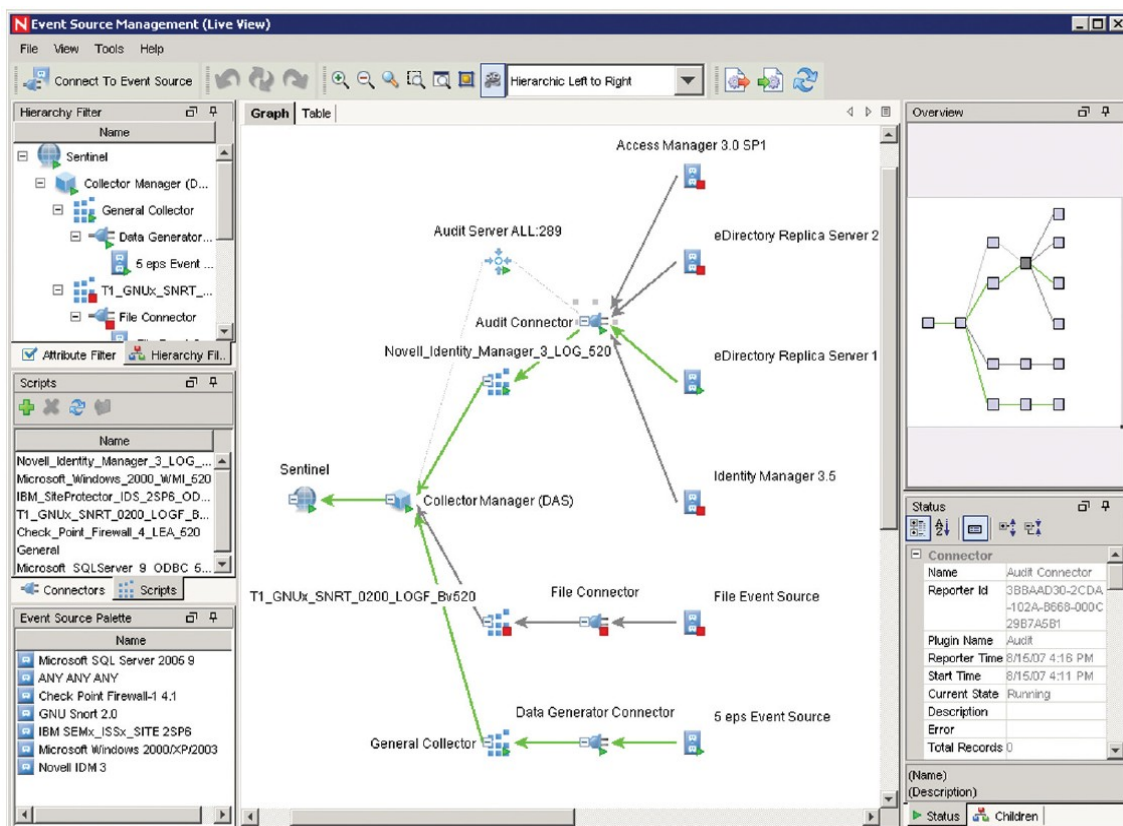
Z wyjątkiem kilku systemów, takich jak komputery typu mainframe, kolektory nie korzystają z agentów. Umożliwia to zdalne gromadzenie danych bez konieczności instalowania jakiegokolwiek oprogramowania w monitorowanym systemie czy urządzeniu.

Zarządzanie źródłami zdarzeń

Novell Sentinel Log Manager wyposażony jest w scentralizowany mechanizm zarządzania źródłami danych o zdarzeniach, ułatwiający integrację źródeł danych. Umożliwia on dokonywanie wszelkich czynności związanych z konfigurowaniem, wdrażaniem, zarządzaniem i monitorowaniem kolektorów danych w różnorodnych systemach. Umożliwia on zarządzanie i monitorowanie wszystkich połączeń między rozwiązaniem Novell Sentinel Log Manager i jego źródłami danych.

Mechanizm ten zbiera dane z systemów źródłowych, przetwarza je i udostępnia informacje o zdarzeniach do celów dalszej analizy, wizualizacji i raportowania, wykorzystując następujące komponenty i funkcje:

- **Kolektory.** Dokonują rozbioru i normalizacji danych o zdarzeniach z różnych systemów
- **Taksonomia.** Umożliwia spójną kategoryzację danych z różnorodnych źródeł
- **Filtrowanie.** Eliminuje nieistotne dane w miejscu ich gromadzenia, zmniejszając obciążenie sieci i przestrzeni dyskowej
- **Istotność biznesowa.** Umożliwia wzbogacenie danych o zdarzeniach o cenne informacje o środowisku, np. atrybuty zasobów
- **Normalizacja.** Wykorzystując metatagi, sprowadza dane do standardowego formatu, umożliwiając ich korelację i raportowanie



Rys. 5. Ogromne możliwości zarządzania źródłami danych o zdarzeniach

Kanały

Jako część usługi gromadzenia danych, architektura magistrali komunikatów tworzy niezależne, wielokanałowe środowisko, które praktycznie eliminuje konflikty i umożliwia równoległe przetwarzanie zdarzeń. Kanały te i podkanały służą nie tylko do przesyłania danych o zdarzeniach, ale i umożliwiają precyzyjne sterowanie procesami, wykorzystywane przy skalowaniu i równoważeniu obciążeń systemu przy zmiennym obciążeniu.

Usługi dostępu do danych

Usługi dostępu do danych powiązane są z magistralą komunikatów i realizują szereg funkcji porządkowych, takich jak weryfikacja, czy zalogowani użytkownicy mają odpowiednie uprawnienia do dostępu bądź tworzenia raportów w oparciu o określone porcje danych. Obsługują również konfigurację portów umożliwiających odbieranie danych z różnych źródeł.

Sentinel Link

Sentinel Link umożliwia hierarchiczne łączenie wielu systemów Sentinel, w tym Sentinel Log Manager i dwóch systemów Sentinel jako rozwiązań klasy SIEM – Novell Sentinel i Novell Sentinel Rapid Deployment (RD).

Sentinel Link zapewnia wiele korzyści, m.in.:

- *Kilka systemów Sentinel Log Manager można połączyć w sposób hierarchiczny. Miejscowe bądź rozproszone serwery Sentinel Log Manager mogą zarządzać dużą ilością danych, zachowując lokalnie nieprzetworzone dane i dane o zdarzeniach, a informacje o ważnych zdarzeniach przesyłając do centralnego systemu Log Manager w celu konsolidacji.*
- *Jeden lub kilka systemów Sentinel Log Manager może przekazywać dane do systemów SIEM – Sentinel lub Sentinel RD. Umożliwiają one wizualizację danych w czasie rzeczywistym, ich zaawansowaną korelację, zarządzanie przekazywaniem zadań oraz integrację z systemami zarządzania tożsamością.*

Składowanie zdarzeń bieżących

Wszystkie dane o zdarzeniach gromadzone przez Sentinel Log Manager są początkowo składowane w pamięci masowej rozwiązania. W odróżnieniu od konkurencyjnych rozwiązań, Sentinel Log Manager wykorzystuje standardowe systemy pamięci masowej. Może korzystać z lokalnego systemu dyskowego serwera lub używać dołączonego systemu SAN lub NAS w celu rozszerzenia przestrzeni dyskowej. Oprócz tego, aby zminimalizować zapotrzebowanie na pamięć masową, rozwiązanie automatycznie kompresuje dane w stosunku 10:1.

Większość dostawców rozwiązań do zarządzania rejestrami zdarzeń wykorzystuje nietypowe systemy składowania danych, co nie tylko podnosi koszty, ale jest przyczyną szeregu innych problemów, takich jak zależność od określonych narzędzi do raportowania i wyszukiwania, niemożność analizowania zarchiwizowanych danych bez ich powtórnego przeniesienia na urządzenia tego dostawcy oraz trudności z udowodnieniem, że takie dane nie zostały zmodyfikowane. Novell Sentinel Log Manager używa standardowych pamięci masowych i stosuje sygnatury danych, gwarantujące spójność rejestrów, co eliminuje owe problemy.

Oto główne aspekty składowania danych bieżących przez Novell Sentinel Log Manager:

- *Nieprzetworzone dane*
- *Zdarzenia*
- *Indeks zdarzeń*
- *Polityki składowania*

Nieprzetworzone dane

Choć kolektory wzbogacają gromadzone dane o zdarzeniach o dodatkowe metadane (taksonomię i istotność biznesową), które ułatwiają identyfikację i klasyfikację zdarzeń, rozwiązanie przechowuje również nieprzetworzone dane o zdarzeniach bieżących. Format nieprzetworzonych danych zależy od konektora i źródła zdarzenia, ale zazwyczaj zawierają one informacje o nieprzetworzonym komunikacie, identyfikator rekordu zawierającego nieprzetworzone dane, czas ich otrzymania, źródło zdarzenia, identyfikatory kolektora i węzła menedżera kolektora, sumę kontrolną nieprzetworzonych danych według SHA-256 itd.

Novell Sentinel Log Manager przechowuje nieprzetworzone dane w sposób gwarantujący, że nie zostały one zmodyfikowane. Przechowywanie danych w postaci nieprzetworzonej pomaga spełnić wymagania przepisów wprowadzone dla ułatwienia dochodzeń i procesów sądowych. Oczywiście, nieprzetworzone dane są skompresowane dla zminimalizowania ich objętości.

Zdarzenia

Aby zwiększyć użyteczność zgromadzonych danych, Novell Sentinel Log Manager dołącza do nieprzetworzonych danych formatowanie, przekształcając je w strukturę informacyjną o zdarzeniu. Struktury te zawierają metadane o taksonomii, normalizacji i istotności biznesowej, ułatwiające osobom odpowiedzialnym za zapewnianie zgodności z przepisami i bezpieczeństwo zrozumienie i możliwość wykorzystania zebranych informacji. Podobnie jak nieprzetworzone dane, struktury te są przechowywane w kompresji w pamięci masowej dla zdarzeń bieżących.

Indeks zdarzeń

Novell Sentinel Log Manager indeksuje wszystkie przechowywane informacje o zdarzeniach, aby ułatwić przeszukiwanie zebranych danych i tworzenie raportów. W celu przyspieszenia wyszukiwania indeksy są przechowywane bez kompresji.

Polityki składowania

Novell Sentinel Log Manager umożliwia konfigurowanie polityk przechowywania danych i określanie, jak długo informacje o określonych zdarzeniach mają być składowane online przed przeniesieniem do archiwum i kiedy mają zostać usunięte.

Składowanie zdarzeń archiwalnych

W miarę upływu czasu, stare dane o zdarzeniach muszą być przenoszone do archiwum. Archiwum Novell Sentinel Log Manager wykorzystuje skompresowany system plików *squashfs* dostępny w SUSE Linux Enterprise Server 11, co odróżnia go od konkurencyjnych rozwiązań w dwóch obszarach. Po pierwsze, Novell Sentinel Log Manager i *squashfs* pozwalają korzystać z zewnętrznych pamięci masowych, które mogą być montowane za pomocą NFS lub CIFS. Oznacza to brak konieczności inwestowania w drogie urządzenia archiwizacyjne i możliwość wykorzystania istniejących, standardowych pamięci masowych, takich jak SAN lub NAS. Po drugie, Novell Sentinel Log Manager umożliwia wykonywanie zapytań i tworzenie raportów w oparciu o dane przechowywane w archiwum. W przypadku większości innych rozwiązań do zarządzania rejestrami zdarzeń wymagałoby to pracochłonnego przywrócenia danych z archiwum. Dzięki możliwości montowania woluminów archiwalnych, Novell Sentinel Log Manager jest w stanie wykonywać zapytania i tworzyć raporty w oparciu zarówno o dane bieżące, jak i archiwalne.

Oprócz tego, Novell Sentinel Log Manager jest w stanie określić w oparciu o kryteria wyszukiwania, czy danych o zdarzeniu należy szukać online, czy w archiwum. Wszystkie te zalety znacznie upraszczają i przyspieszają działania związane z zapewnianiem zgodności z wymogami przepisów.

Pamięć konfiguracji

Podczas gdy nieprzetworzone dane o zdarzeniach, struktury informacji o zdarzeniach i indeksy przechowywane są w postaci plików, Novell Sentinel Log Manager przechowuje informacje konfiguracyjne, informacje związane z zarządzaniem użytkownikami oraz raporty i szablony raportów w bazach danych PostgreSQL.

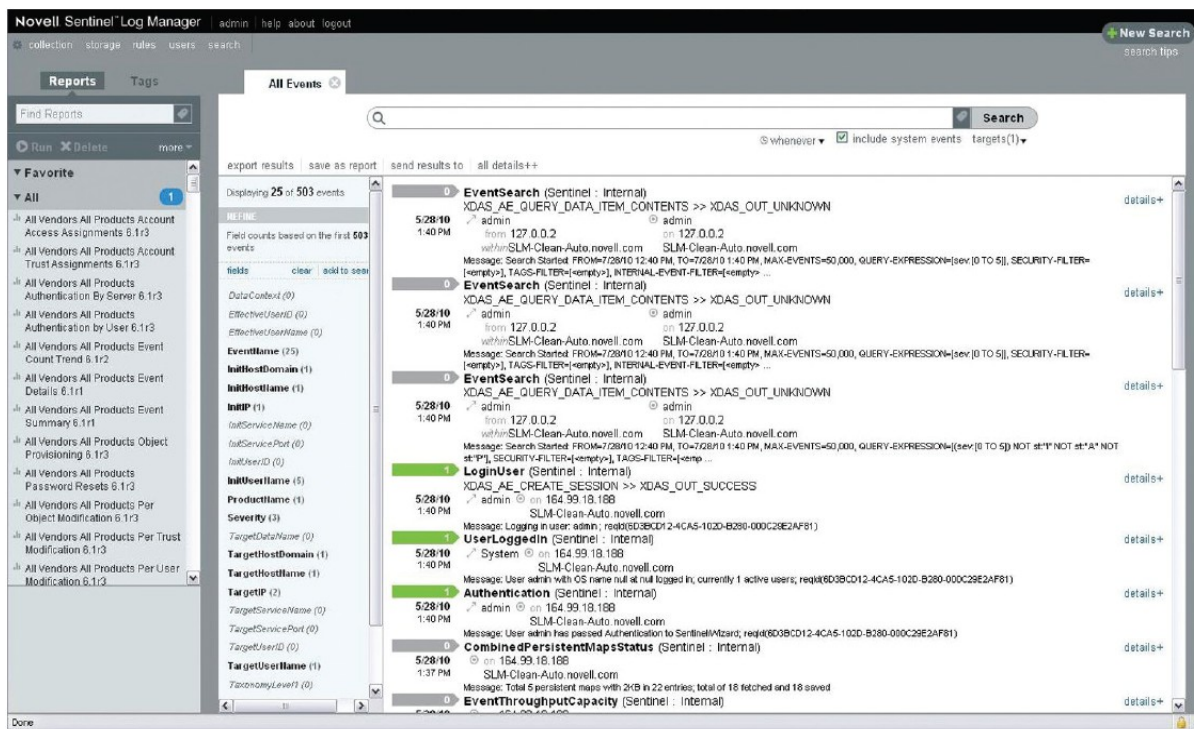
Usługi zdarzeń

Usługi zdarzeń w Novell Sentinel Log Manager realizują funkcje wyszukiwania i raportowania.

Usługi wyszukiwania

Novell Sentinel Log Manager udostępnia potężne, pełnotekstowe funkcje wyszukiwania w zgromadzonych rejestrach zdarzeń, zarówno przechowywanych online, jak i w archiwum. Korzystając z funkcjonalnego silnika wyszukiwania opartego na Lucene i interfejsu internetowego Ajax, użytkownicy mogą inicjować wyszukiwanie z dowolnego z ekranów rozwiązania, a jego wyniki ukażą się niemal natychmiast w nowej zakładce.

W przeciwieństwie do innych rozwiązań, które przestają reagować na działania użytkownika do chwili zakończenia wyszukiwania (co może trwać godziny, a nawet dni, w zależności od wielkości zbioru danych) lub wyświetlają jedynie ograniczoną ilość danych (co wymusza wielokrotne klikanie w celu zobaczenia kolejnych stron wyników), Novell Sentinel Log Manager wyświetla wyniki od razu po ich znalezieniu. Takie działanie umożliwia dynamiczną interakcję z użytkownikiem.



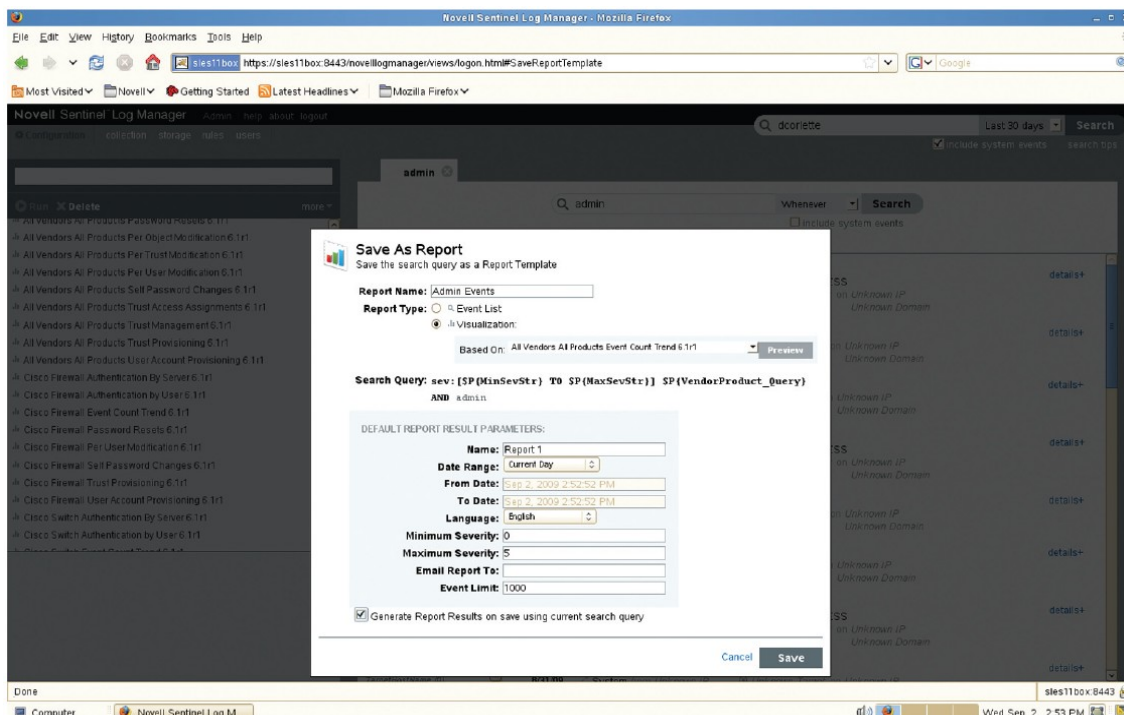
Rys. 6. Wyszukiwanie rozproszone

Dynamiczny charakter interfejsu wyszukiwania nie tylko umożliwia przerwanie wyszukiwania w dowolnym momencie, ale i zmianę jego kryteriów „w locie”. Jeśli na przykład użytkownik dojdzie do wniosku, że wyszukiwanie daje zbyt wiele wyników, może kliknąć pole zdarzenia odpowiadające typowi szukanej informacji (np. adres IP, rodzaj uwierzytelnienia, rodzaj systemu operacyjnego, użytkownika itp.), a nowe kryterium zostanie natychmiast dodane do filtra wyszukiwania i na odświeżonym ekranie ukażą się tylko zawężone wyniki. Kryteria wyszukiwania można modyfikować zarówno w jego trakcie, jak i po jego zakończeniu.

Ponieważ Novell Sentinel Log Manager przechowuje dane o zdarzeniach oraz indeksy w płaskich plikach, Novell zoptymalizował mechanizm wyszukiwania pod kątem takiego formatu. Pozwoliło to znacznie przyspieszyć wyszukiwanie w stosunku do innych rozwiązań do zarządzania rejestrami zdarzeń, które do przechowywania informacji wykorzystują bazy danych. Przechowywanie nieprzetworzonych danych, informacji o zdarzeniach i indeksów w płaskich plikach umożliwia zharmonizowanie działania usług wyszukiwania i raportowania, co znacznie zwiększa ich szybkość i efektywność. Aby zobaczyć szczegółowe informacje na temat dowolnego ze znalezionych zdarzeń, wystarczy kliknąć odpowiedni odnośnik na stronie wyników. Interfejs umożliwia również przeglądanie nieprzetworzonych danych powiązanych ze znalezionymi zdarzeniami. Jedną z najbardziej przydatnych cech wyszukiwarki Novell Sentinel Log Manager jest możliwość zapisania wyników w postaci prostego raportu lub szybkiego przekształcenia wyników wyszukiwania w wyrafinowany, sformatowany raport.

Usługi raportowania

Podczas gdy wszystkie raporty w Novell Sentinel Log Manager wykorzystują zawarte w rozwiązaniu elastyczne i funkcjonalne możliwości wyszukiwania, usługi raportowania udostępniają dwa rodzaje raportów. Pierwszy to raport z wyszukiwania, gdzie użytkownik wprowadza kryteria, a Novell Sentinel Log Manager zwraca wyniki w formacie prostej listy. Ta postać zazwyczaj spełnia wymagania w stosunku do raportów tworzonych na potrzeby prostych audytów czy też weryfikacji zgodności z wymogami przepisów.



Rys. 7. Dla otrzymania raportu z wyników wyszukiwania wystarczy jedno kliknięcie

Drugi rodzaj ma postać bardziej formalną i daje większe możliwości dostosowania do określonych wymagań. Za pomocą jednego kliknięcia Novell Sentinel Log Manager może przekształcić raport z wyszukiwania w formalną prezentację, ukazującą określone pola i parametry wymagane często w raportach zgodności z wymogami przepisów czy raportach tworzonych na potrzeby audytów. Novell Sentinel Log Manager udostępniła szeroką gamę szablonów formatowania, za pomocą których lista wyników wyszukiwania może być automatycznie przekształcona na wybrany format, odpowiadający określonym wymaganiom.



Rys. 8. Przejrzyste raporty pozwalają zapomnieć o problemach z udowodnieniem zgodności z przepisami

Szablony zawarte w Novell Sentinel Log Manager obejmują na przykład raporty ukazujące próby modyfikacji praw dostępu, przydzielania i odbierania uprawnień, zmian skojarzenia praw, tworzenia i usuwania kont, próby modyfikacji atrybutów kont, modyfikacji danych, zmiany haseł użytkowników przez administratorów, próby uwierzytelniania przez użytkowników itd. Novell Sentinel Log Manager umożliwia także dostosowanie istniejących i tworzenie nowych szablonów.

Mechanizm raportowania Novell Sentinel Log Manager może również interpretować dane pochodzące z szerokiego spektrum źródeł bez konieczności żmudnego dostosowywania. Novell Sentinel Log Manager zawdzięcza możliwość przekształcania wyników wyszukiwania w raporty faktowi wykorzystania do obu celów tych samych zestawów danych.

Oprócz przekształcania wyników wyszukiwania w formalne raporty, istnieje także możliwość automatycznego generowania raportów według zdefiniowanego harmonogramu. Zaplanowane raporty mogą być wysyłane pocztą elektroniczną do określonych użytkowników lub grup. Wszystkie raporty, zarówno tworzone na żądanie (*ad hoc*), jak i według harmonogramów, można zapisać do późniejszego wykorzystania.

Możliwość przekształcania wyników wyszukiwania w raporty za pomocą szablonów daje rozwiązaniu Novell Sentinel Log Manager wyraźną przewagę nad gotowymi szablonami raportów używanymi przez inne rozwiązania, które przed użyciem wymagają zazwyczaj pracochłonnego skonfigurowania i dostosowania kryteriów oraz pól. Sporo pracy wymaga też zwykle wykorzystanie szablonów innych producentów do tworzenia raportów według konkretnych wymagań w oparciu o różnorodne źródła danych.

Krótko mówiąc, obecne w Novell Sentinel Log Manager indeksowanie danych i możliwość tworzenia raportów za jednym kliknięciem ogromnie upraszczają działania związane z generowaniem raportów na potrzeby audytów i dokumentowania zgodności z wymogami przepisów.

Zgodność z przepisami – prosto, inteligentnie i ekonomicznie

Novell Sentinel Log Manager udostępni możliwość inteligentnego gromadzenia, agregowania, składowania, analizowania i zarządzania rejestrami zdarzeń z wszelkich posiadanych systemów i aplikacji, aby ułatwić firmom zapewnianie zgodności z wymogami przepisów państwowych i branżowych. Rozwiązanie wykorzystuje sprawdzoną architekturę integracji danych Novell Sentinel wraz z szeroką gamą kolektorów dla baz danych, systemów operacyjnych, usług katalogowych, firewalli, systemów wykrywania i przeciwdziałania włamaniom, programów antywirusowych, komputerów klasy mainframe, serwerów witryn i aplikacji internetowych itd. Rozwiązanie wykorzystuje indeksowanie danych i mechanizm tworzenia raportów za jednym kliknięciem, znacznie upraszczając tworzenie raportów na potrzeby audytów i dokumentowania zgodności z wymogami przepisów. Zdolność do montowania woluminów archiwalnych pozwala bez problemu przeszukiwać dane bieżące i archiwalne i wykorzystywać je do tworzenia raportów, co radykalnie ułatwia i przyspiesza zadania związane z zapewnianiem zgodności z przepisami.

Novell Sentinel Log Manager to elastyczne i łatwe w użyciu rozwiązanie do zarządzania rejestrami zdarzeń, otwierające prostą drogę do kompletnych rozwiązań SIEM (*Security Information & Event Management*) czasu rzeczywistego. Wykorzystując doświadczenia Novella w zakresie SIEM, Sentinel Log Manager ułatwia spełnianie wymagań przepisów i pozwala bez ponoszenia nadmiernych kosztów zbudować solidny fundament dla aktywnego ograniczania ryzyka.

Więcej informacji na temat Novell Sentinel Log Manager można znaleźć pod adresem www.novell.com/products/sentinel-log-manager

W celu uzyskania szczegółowych informacji o cenach i licencjonowaniu prosimy kontakt:

Novell Sp. z o.o.
ul. Postępu 21
02-676 Warszawa
tel. 0 22 537 5000
bezpłatna infolinia 0 800 22 66 85
infolinia@novell.pl