

HP Service Health Analyzer: rozszyfrowywanie struktury (DNA) problemów z wydajnością infrastruktury informatycznej

Oficjalny dokument techniczny

Spis treści

Wprowadzenie.....	2
Unikatowe podejście firmy HP — narzędzie HP SHA oparte na rozwiązaniu HP Run-time Service Model2	
HP SHA — analiza prognostyczna w czasie przetwarzania	5
Możliwości produktu	6
Rozpoczęcie pracy z produktem bez konieczności jego konfigurowania i utrzymywania	7
Zwrot z inwestycji.....	12
Podsumowanie.....	12



Wprowadzenie

We współczesnych środowiskach opartych na przetwarzaniu w chmurze i zwirtualizowanych systemach informatycznych posiadanie pełnej wiedzy o stanie usług biznesowych, którą można wykorzystać i dzięki której można przetrwać na rynku, to nie tylko miły dodatek. To prawdziwa konieczność. Zarządzanie zmieniającą się strukturą i aplikacjami nie polega wyłącznie na reagowaniu na problemy z usługami biznesowymi, które już wystąpiły, ani na ręcznym aktualizowaniu statycznych wartości progowych, które są trudne do precyzyjnego określenia i kłopotliwe w utrzymaniu.

W dzisiejszym świecie niezbędne jest powiadomienie o problemach z odpowiednim wyprzedzeniem, aby można było rozwiązać je, zanim zaszkodzą działalności biznesowej. Potrzebny jest lepszy wgląd w sposób korelowania aplikacji i usług biznesowych ze zmieniającą się infrastrukturą, który umożliwi monitorowanie anomalii w całym środowisku informatycznym obejmującym sieć, serwery, oprogramowanie pośredniczące, aplikacje i procesy biznesowe. W łatwiejszy sposób musi odbywać się określanie dopuszczalnych wartości progowych stanowiących podstawę do wykrywania zdarzeń, które mogą wpłynąć na działalność biznesową. Konieczne jest zautomatyzowanie działań, które pozwoli na wykorzystanie wiedzy o wcześniejszych zdarzeniach do skuteczniejszego rozwiązywania nowych problemów, a także do ochrony przed problemami zewnętrznymi, co pozwoli pracownikom działów informatycznych skoncentrować się wyłącznie na zdarzeniach mających wpływ na działalność biznesową.

Wprowadzie działy informatyczne organizacji dysponują metodami gromadzenia ogromnych ilości danych, jednak brakuje im zestawu narzędzi analitycznych oraz systemów sztucznej inteligencji, które umożliwiłyby skorelowanie poszczególnych metryk widzianych z perspektywy aplikacji i topologii w celu przewidywania potencjalnych problemów, zanim one wystąpią. Menedżerowie działów informatycznych zaczynają interesować się światem analizy prognostycznej (jednego z wartych uwagi trendów w analizie biznesowej w 2011 r.), mając nadzieję, że pomoże im ona poprawić ciągłość i wydajność świadczenia usług, zwiększając w ten sposób zyski generowane przez działalność biznesową oraz zmniejszając koszty utrzymania i obsługi.

Rozwiązanie HP Service Health Analyzer (SHA) to narzędzie do analizy prognostycznej bazujące na dynamicznym modelu usług czasu rzeczywistego, które umożliwia zrozumienie związków, jakie zachodzą między odstępstwami od normy w zachowaniu metryk a aplikacjami i infrastrukturą bazową.

Unikatowe podejście firmy HP — narzędzie HP SHA oparte na rozwiązaniu HP Run-time Service Model

Systemy monitorowania podają informacje o pomiarach i zdarzeniach ze wszystkich warstw infrastruktury informatycznej — sprzętu, sieciowego systemu operacyjnego, oprogramowania pośredniczącego, aplikacji, usług i procesów biznesowych. Bazy danych zarządzania konfiguracją (CMDB) zapewniają model łączący te wszystkie zróżnicowane składniki. Jednak ze względu na nieustannie zmieniającą się naturę systemów informatycznych bazy danych CMDB wymagają stałego aktualizowania. Dzieje się tak również w przypadku rozwiązania HP Run-time Service Model (RtSM). Opisane powyżej wymagania spełnia dopiero połączenie monitorów i bazy danych CMDB działającej w czasie rzeczywistym, które zapewnią wszystkie niezbędne dane. Wymagają one jednak przekształcenia na postać zawierającą przydatne informacje. W aplikacji HP SHA zastosowano aparat do wykrywania anomalii w czasie przetwarzania (RAD) zawierający zaawansowane algorytmy, które łączą różne dyscypliny, topologię, analizy danych, teorię wykresów i statystyki.

Rozwiązanie RtSM jest odpowiedzią firmy HP na przestarzały model usług. RtSM synchronizuje się z produktem HP UCMDB w celu wykorzystania modelowania usług w „zewnętrznej” uniwersalnej bazie danych konfiguracji (UCMDB, Universal Configuration Management Database). Następnie za pomocą dostępnych w rozwiązaniu HP Business Service Management (Business Service Management) modułów zbierających dane monitoruje wydajność, dostępność, usterki i topologię w celu udostępnienia topologii w czasie rzeczywistym, aby aparat RtSM dysponował najświeższą wiedzą o topologii i zachodzących relacjach. RtSM to rdzeń rozwiązania SHA.

Więcej informacji na temat sposobu współpracy rozwiązania RtSM z bazą danych UCMDB zawiera dokument „[Wskazówki dotyczące najlepszych sposobów postępowania z aparatem RtSM](#)”

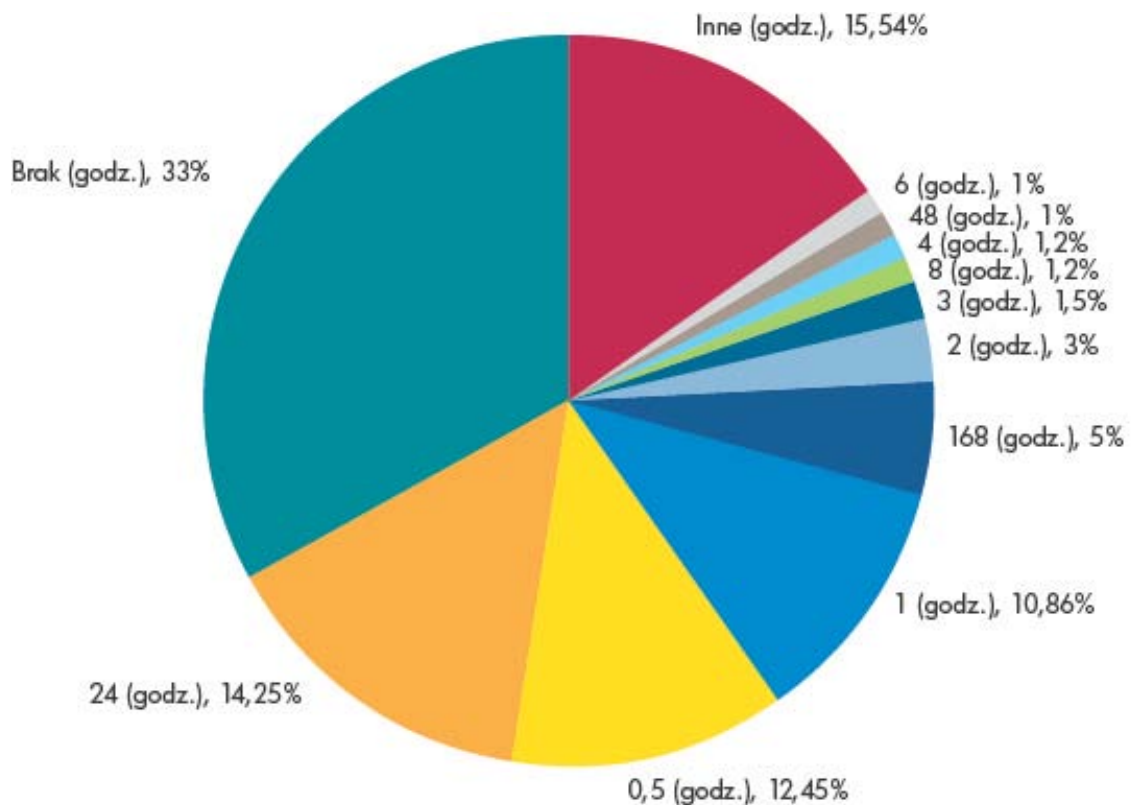
Rysunek 1. Szablon rozwiązania



Rysunek 1 przedstawia składniki rozwiązania SHA, które naszym zdaniem są niezbędne do precyzyjnego wykrywania problemów z wydajnością infrastruktury informatycznej. Poniżej znajduje się opis składników i ich wymagań.

Tworzenie poziomów odniesienia to pierwszy składnik, który pobiera wszystkie metryki gromadzone przez systemy monitorowania i uczy się ich normalnego zachowania. Odchylenia od normalnego zachowania metryk stanowią pierwszy krok do wykrywania, przewidywania i rozszyfrowywania problemów z wydajnością. Jednak dokładne poznanie normalnego zachowania metryk nie jest łatwym zadaniem. Takie czynniki jak zachowanie sezonowe, trendy i zmiany powodowane przez stale ewoluujący system informatyczny wymagają, aby algorytm uczenia się szacujący poziom odniesienia był elastyczny i uwzględniał te czynniki. Rysunek 2 przedstawia rozkład sezonu dla ponad 17 000 metryk wydajności zebranych z rzeczywistego systemu informatycznego. Są one kombinacją monitorów systemu, monitorów aplikacji i monitorów na poziomie użytkownika. Jak widać na rysunku, ponad dwie trzecie metryk wykazuje jakieś zachowania sezonowe, przy czym dotyczą one różnych sezonów, a nie tylko zakładanej zazwyczaj sezonowości dziennej lub tygodniowej. Algorytm poziomu odniesienia najpierw musi precyzyjnie oszacować sezon. Jeśli metryka charakteryzuje się zachowaniem sezonowym w okresie pięciu godzin, a algorytm poziomu odniesienia ignoruje ten sezon lub używa wstępnie zdefiniowanego sezonu, który jest niepoprawny (na przykład 24-godzinnego), utworzony poziom odniesienia jest nieprawidłowy. Poziom odniesienia jest zbyt wrażliwy, powodując liczne fałszywe odchylenia od normy, które w rzeczywistości mieszczą się w normie, lub też jest zbyt obojętny i nie wykrywa odstępstw od normalnego zachowania, gdy takie odstępstwa występują.

Rysunek 2. Rozkład zachowania sezonowego dla ponad 17 000 metryk zebranych ze środowiska informatycznego



Równie ważne w procesie szacowania dobrego poziomu odniesienia jest szacowanie trendów i dostosowywanie się do zmian.

Wiedza na temat normalnego zachowania poszczególnych metryk jest ważna, ale niewystarczająca do wykrywania i przewidywania rzeczywistych problemów. Z definicji niektóre odchylenia od poziomu odniesienia nie są związane z żadnym problemem (niewielki ułamek). W dużym środowisku informatycznym gromadzącym miliony metryk nawet ten mały ułamek może prowadzić do występowania zbyt wielu fałszywych alarmów, jeśli każde z tych odchyłeń z osobna zostanie potraktowane jako problem. Ponadto problemy zazwyczaj przejawiają się w więcej niż jednej metryce w środowisku.

Analiza czasowa: To jedna z najbardziej rozpowszechnionych metod łączenia metryk w pojedynczą anomalię. Do metod analizy czasowej należą korelacje między metrykami, w których metryki są grupowane ze sobą na podstawie podobieństwa ich pomiarów w seriach czasowych, oraz wielowymiarowa analiza/prognoza czasowa, która łączy ze sobą wiele metryk za pomocą zazwyczaj liniowego, wielowymiarowego modelu matematycznego, na przykład modelu regresji wielowymiarowej, modelu neuronowego lub modelu Bayesa.

Metody te są skuteczne, ale mają pewne ograniczenia. Przede wszystkim słabo poddają się skalowaniu w przypadku wielu metryk. Poza tym ze względu na swoją statystyczną naturę mogą powodować odnajdywanie błędnych korelacji, gdy otrzymają ogromną liczbę metryk, między którymi nie ma żadnych rzeczywistych związków. Szansa znajdowania tego rodzaju błędnych korelacji rośnie wraz z liczbą metryk.

Analiza topologii: W pokonaniu ograniczeń metod czasowych pomaga kontekst związany z dziedziną. Szczególnie w środowiskach informatycznych zestaw analizowanych metryk należy ograniczyć do logicznego zestawu metryk, które są ze sobą powiązane. Jeśli stopień wykorzystania procesorów dwóch zupełnie niezwiązanych ze sobą serwerów rośnie w tym samym czasie, nie należy doszukiwać się korelacji między nimi, nawet jeśli z punktu widzenia statystyki taka korelacja istnieje. Tego rodzaju kontekst w topologii systemów informatycznych zapewniają bazy danych CMDB. CMDB to zasadniczo wykres przedstawiający model relacji między wszystkimi składnikami systemów informatycznych — warstwą fizyczną oraz warstwami oprogramowania pośredniczącego, programów, aplikacji, usług biznesowych i procesów. Z tego względu analiza topologii w postaci zaawansowanych algorytmów tworzenia wykresów jest niezbędna do wyodrębniania informacji kontekstowych w bazie danych CMDB oraz ułatwia wykrywanie rzeczywistych problemów i korelacji między metrykami, odfiltrując niepotrzebne informacje.

Wykrycie rzeczywistego problemu polega więc na odkryciu wzorców odstępstw od normy wielu metryk w określonym czasie i odfiltrowaniu ich według topologii. Prowadzi to do uzyskania metod uczenia się na bazie statystyki analizujących dane czasowe i dane topologiczne.

Analiza danych historycznych: Oprócz wykrywania i przewidywania problemów topologia umożliwia określanie problemów i znajdowanie ich głównych przyczyn na podstawie objawów. Obie funkcje są równie ważne dla szybkiego rozwiązywania problemów. Po wykryciu i przeanalizowaniu problemu następuje ostateczne rozszyfrowanie jego wzorca struktury DNA, który można zapisać w bazie wiedzy. Do korzystania z bazy wiedzy niezbędne są algorytmy przeprowadzające analizę danych historycznych. Należą do nich algorytmy technik dopasowywania i porównywania wzorców DNA różnych problemów, ich grupowania i klasyfikowania. Baza wiedzy w połączeniu z algorytmami umożliwia szybkie i automatyczne diagnozowanie problemów, które występowały już wcześniej, oraz ułatwia znajdowanie głównych przyczyn i rozwiązań nowych problemów.

Aparat RAD: Na jego definicję składa się pełen zestaw powyższych algorytmów. Algorytmy zawarte w aparacie RAD są przedmiotem 12 oddzielnych wniosków patentowych. Aparat RAD generuje dane wyjściowe w postaci krytycznego kluczowego wskaźnika wydajności (KPI) na pulpicie nawigacyjnym produktu HP BSM oraz wysyła informacje o zdarzeniu do podsystemu zdarzeń produktu BSM, który nosi nazwę HP Operations Manager i (OMi). Zdarzenie z produktu SHA zawiera mnóstwo informacji kontekstowych zgromadzonych przez aparat RAD, między innymi informacje o głównych podejrzanych, lokalizacji i wpływie na działalność biznesową, listę elementów konfiguracji (CI), których dotyczy anomalia, oraz wszystkie podobne informacje o anomaliach. Informacje te pozwalają klientom na szybkie diagnozowanie i rozwiązywanie problemów, zanim zaszkodzą one działalności biznesowej.

HP SHA — analiza prognostyczna w czasie przetwarzania

W ramach produktu SHA opracowaliśmy algorytmy uczenia się na bazie statystyki, które w połączeniu z algorytmami tworzenia wykresów umożliwiają analizowanie pełnego zakresu danych zebranych przez systemy BSM, takich jak:

- Dane monitorowania (syntetyczne i dotyczące rzeczywistych użytkowników)
- Zdarzenia
- Zmiany
- Topologia z rozwiązania RISM

Algorytmy te precyzyjnie wykrywają anomalie, rozszyfrowują ich strukturę DNA, oceniają ich wpływ na działalność biznesową i dopasowują je do rozszyfrowanych wcześniej anomalii zgromadzonych w naszej bazie wiedzy o strukturze DNA anomalii.

Rozwiązanie SHA można opisać w kilku punktach:

- **Uczenie się zachowania metryk**

Pierwszą niezbędną czynnością jest nauczenie się normalnego zachowania (nazywane także tworzeniem poziomów odniesienia) metryk zebranych ze wszystkich poziomów usługi (systemu, oprogramowania pośredniczącego, aplikacji itp.). Eliminuje ona konieczność określania statycznych wartości progowych i umożliwia wczesne wykrywanie odstępstw od normy. Największe atuty naszych algorytmów to:

- **Automatyczne** uczenie się sezonowego zachowania metryk i jego trendu
- **Dostosowywanie się** do zmian zachowania w czasie — niezbędne w środowiskach zwirtualizowanych
- **Brak konieczności konfigurowania** — określanie i utrzymywanie wartości progowych nie wymaga wysiłku ze strony administratorów

- **Technologia Anomali DNA — wykrywanie**

W miarę ewoluowania problemu holistycznego w usłudze informatycznej liczne metryki i składniki związane z tą usługą zaczynają wykazywać odchylenia od normalnego zachowania. Jednak w przypadku różnych składników występują stałe, chwilowe odstępstwa od normy, które nie oznaczają żadnego poważnego problemu. Wyzwaniem dla każdego systemu wykrywania anomalii jest wyselekcjonowanie poważnych problemów i odkrycie struktury DNA prawdziwych problemów. Nasz algorytm wykrywania struktury DNA anomalii wykonuje te zadania, stosując unikatowy algorytm statystyczny, który łączy trzy rodzaje informacji niezbędnych do osiągnięcia dokładności wykrywania:

- **Informacje topologiczne:** łączy logiczne między monitorami i monitorowanymi przez nie składnikami
- **Informacje czasowe:** czas trwania i korelacja czasowa monitorów znajdujących się w stanie odchylenia od normalności
- **Informacje o pewności statystycznej:** prawdopodobieństwo, że monitor naprawdę znajduje się w stanie odstępstwa od normy, na podstawie poziomów odniesienia określonych w czasie

Największe atuty naszego algorytmu wykrywania anomalii to:

- **Ograniczenie ilości nieistotnych informacji:** Oferuje automatyczną metodę grupowania metryk, które przekroczyły swoje poziomy odniesienia, za pomocą informacji czasowych i topologicznych. To z kolei powoduje zmniejszenie liczby zdarzeń przekroczenia poziomów odniesienia, którymi musiałby się zająć operator, bez konieczności określania jakichkolwiek reguł.
- **Ograniczenie liczby zdarzeń:** Algorytm rozwiązania SHA łączy wiele metryk wykazujących odstępstwa od normy w jedno zdarzenie, zmniejszając łączną liczbę zdarzeń przedstawianych operatorowi. Punktem wejścia tego typu zdarzenia jest wiele metryk przekraczających swoje dynamiczne wartości progowe. W takiej sytuacji rozwiązanie SHA koreluje te metryki na podstawie czasu i topologii w celu wygenerowania pojedynczego zdarzenia umożliwiającego operatorowi skoncentrowanie się na rzeczywistym problemie.
- **Ograniczenie liczby fałszywych alarmów:** Produkt ogranicza liczbę fałszywych alarmów, obliczając znaczenie anomalii dla systemu za pomocą algorytmu statystycznego. Również znane anomalie, które w przeszłości zostały oznaczone jako niegroźne, są używane w celu dopasowania do bieżących anomalii i powstrzymania zdarzenia anomalii.

• **Technologia Anomali DNA — rozszyfrowywanie**

Następnym krokiem po wykryciu anomalii oraz jej struktury jest rozszyfrowanie jej DNA. Rozszyfrowanie struktury DNA anomalii polega na jej przeanalizowaniu i sklasyfikowaniu na podstawie topologii (elementów konfiguracji i ich struktury topologicznej), metryk i dodatkowych informacji. Rozszyfrowanie pozwala w szczególności osiągnąć następujące cele:

- Oddzielenie podejrzanych elementów i dostarczenie w ten sposób przydatnych informacji. Identyfikacja wpływu na działalność biznesową za pomocą informacji dotyczących tej działalności, takich jak: liczba użytkowników, umowy dotyczące poziomu świadczonych usług (SLA) i obszary geograficzne, których dotyczy problem. Dzięki temu możliwe jest nadawanie anomalii priorytetów odpowiadających zagrożeniu.
- Identyfikacja powiązanych zmian, które mogły wpłynąć na zachowanie systemu.

• **Technologia Anomali DNA — dopasowywanie**

Po rozszyfrowaniu struktury DNA anomalii bieżąca anomalia jest dopasowywana do anomalii, które miały miejsce w przeszłości. Dopasowywanie jest przeprowadzane za pomocą unikatowego algorytmu podobieństwa wykresów, który porównuje struktury wyodrębnionych anomalii, umożliwiając w ten sposób dopasowanie między anomaliami wykrytymi w różnych usługach o podobnej architekturze. Nasze dopasowywanie ma następujące zalety:

- Umożliwia wielokrotne użycie opracowanych rozwiązań zdarzeń, które miały miejsce w przeszłości.
- Dopasowuje anomalie do anomalii znanych problemów, które wymagają jeszcze rozwiązania, eliminując konieczność ponownego przeprowadzania tych samych badań.
- Ogranicza liczbę fałszywych alarmów, gdy podobna anomalia z przeszłości została sklasyfikowana jako niegroźna struktura DNA, na przykład anomalia wynikająca z wykonywania zwykłych czynności serwisowych w usługach.

• **Baza wiedzy o strukturze DNA anomalii**

Po zgromadzeniu bazy wiedzy o anomaliach, które miały miejsce w przeszłości, i ich rozwiązaniach można zastosować metody zaawansowanego wyszukiwania danych w celu przeanalizowania i wygenerowania związków między wszystkimi anomaliami, a tym samym utworzenia mapy całej bazy wiedzy o strukturach DNA anomalii. Nasz algorytm dopasowywania struktur DNA anomalii określa wymaganą przestrzeń metryczną dla metod wyszukiwania danych, takich jak grupowanie i klasyfikowanie. Ich zastosowanie przynosi następujące korzyści:

- Proaktywne rozwiązanie problemu — zidentyfikowanie powtarzających się problemów przez zaklasyfikowanie struktur DNA anomalii do różnych typów problemów i rozwiązań skraca czas diagnozowania i rozwiązywania tego typu problemów w przyszłości.
- Wykorzystanie wiedzy zgromadzonej z różnych usług zachowujących się w podobny sposób.

Możliwości produktu

Rozwiązanie HP SHA bazujące na rozwiązaniu HP RtSM analizuje trendy i normy historyczne dotyczące zarówno aplikacji, jak i infrastruktury. Dane te porównuje z metrykami działania systemu w czasie rzeczywistym. Wykorzystanie modelu RtSM ma zasadnicze znaczenie dla zmieniającego się dynamicznie środowiska, ponieważ umożliwia:

- Korelowanie anomalii ze zmianami topologii i problemami, które miały miejsce w przeszłości.
- Ustalanie wpływu poszczególnych problemów na działalność biznesową w celu określenia, które problemy należy rozwiązać w pierwszej kolejności.
- Identyfikowanie prawdopodobnych przyczyn problemu i wykorzystywanie tej wiedzy w celu zapobiegania podobnym problemom w przyszłości.

Produkt SHA automatycznie uczy się dynamicznych wartości progowych w danym środowisku, dzięki czemu nie trzeba tracić czasu na określanie i utrzymywanie statycznych wartości progowych. Rozwiązanie SHA działa w oparciu o metryki pochodzące z następujących źródeł danych BSM:

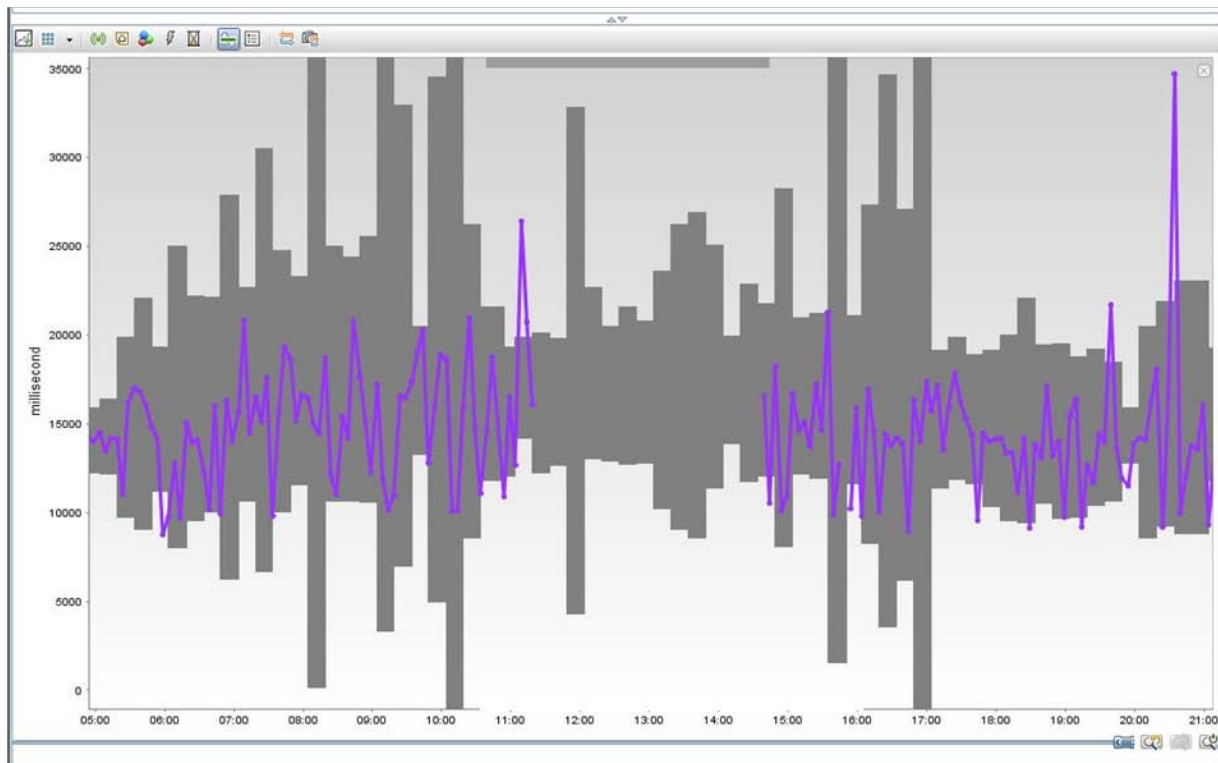
- HP Business Process Monitor
- HP Diagnostics
- HP Network Node Manager i
- HP Operations Manager, Performance Agent
- HP Real User Monitor
- HP SiteScope

Rozwiązanie SHA identyfikuje anomalie na podstawie odbiegającego od normy zachowania metryk ustalonego przez rozwiązanie RtSM, określa kluczowy wskaźnik wydajności (KPI) i generuje zdarzenie z kontekstem ułatwiającym określenie priorytetu biznesowego tego problemu. Dodatkowo w rozwiązaniu SHA zastosowano technologię „DNA anomalii” — Anomaly DNA Technology — do analizowania struktury anomalii i porównywania jej ze znanymi strukturami („DNA”) innych anomalii. Na podstawie wyników tego dopasowywania uzyskuje się informacje o metodzie korygowania problemów bez dodatkowego dochodzenia, a w razie znalezienia dopasowań do zdarzeń oznaczonych jako niegroźne (fałszywe alarmy) powiadomienie o problemie jest tłumione. Jeśli nienormalne działanie jest powiązane z konkretną usługą, można sprawdzić w umowach dotyczących poziomu świadczonych usług (SLA), jaki będzie ewentualny rozmiar konsekwencji wpływu anomalii. Na koniec produkt SHA włącza funkcje korygowania dostępne w rozwiązaniu HP Closed Loop Incident Process (CLIP) i zapewnia bezpośrednią integrację z rozwiązaniem HP Operations Orchestration. Na przykład w celu szybkiego skorygowania problemów można połączyć ze sobą funkcje analizy i automatyzacji. Gdy produkt SHA wysła zdarzenie do rozwiązania OMi, operator może podjąć działania za pomocą procesu CLIP, zanim problem wpłynie na usługę. To rozwiązanie szybkiego korygowania upraszcza obsługę złożonych środowisk wirtualizacji i przetwarzania w chmurze.

Rozpoczęcie pracy z produktem bez konieczności jego konfigurowania i utrzymywania

Po zainstalowaniu produktu należy wybrać aplikacje do monitorowania. Rozwiązanie SHA rozpocznie zbieranie danych i uczenie się zachowania systemu. Rozwiązanie SHA gromadzi dane z aplikacji, infrastruktury, bazy danych, sieci i oprogramowania pośredniczącego oraz informacje dotyczące topologii z rozwiązania RtSM i uczy się poziomu odniesienia. Poziom odniesienia określa normalne zachowanie każdej metryki w czasie, uwzględniając właściwości sezonowe. Na przykład w ramach normalnego zachowania metryki może mieścić się bardzo pracowity poranek w poniedziałek i bardzo spokojne popołudnie w piątek.

Rysunek 3. Przykładowy zakres dynamicznego poziomu odniesienia (w kolorze szarym) z rzeczywistymi danymi metryk (w kolorze fioletowym)



Po ustanowieniu dynamicznych poziomów odniesienia dla wszystkich metryk aplikacji aparat SHA RAD rozpoczyna wyszukiwanie anomalii w zachowaniu aplikacji. Punktem wejścia do aparatu RAD jest przekroczenie poziomu odniesienia oznaczające, że metryka przejawia oznaki zachowania odbiegającego od normy. W celu zdefiniowania anomalii aparat RAD pobiera informacje o odbiegających od normy zachowaniach metryk zgromadzone ze wszystkich monitorowanych metryk i łączy je z informacjami o topologii z rozwiązania RtSM, aby stwierdzić, czy występuje wiele przekroczeń (z różnych metryk) wpływających na tę samą usługę. W przypadku wykrycia anomalii produkt generuje zdarzenie i wysyła je do podsystemu zdarzeń. Ponadto po wykryciu anomalii rozwiązanie SHA automatycznie przechwytuje bieżącą topologię elementów konfiguracji powiązanych z tym zdarzeniem. Ułatwia to zrozumienie topologii aktualnej w momencie wystąpienia anomalii, co jest szczególnie cenne przy przeglądzie anomalii, które wystąpiły w nocy lub w chwili, gdy nie można było skontaktować się z żadnym informatykiem. Ponadto rozwiązanie SHA zbiera i prezentuje informacje o wykrytych zmianach odpowiednich elementów konfiguracji, aby można ich było użyć podczas analizy głównej przyczyny. Ta korelacja oznacza szybsze rozwiązanie problemu i skrócenie średniego czasu naprawy (MTTR).

Gdy rozwiązanie SHA wykrywa anomalie w zachowaniu aplikacji, zmienia stan wskaźnika KPI Predictive Health i wywołuje zdarzenie, które jest wysyłane do przeglądarki zdarzeń BSM. W tym momencie można rozpocząć diagnozowanie problemu i ocenianie jego wpływu na działalność biznesową.

Rozwiązanie SHA udostępnia stronę z informacjami o anomalii, na której znajdują się wszystkie niezbędne dane dotyczące problemu i jego wpływu na działalność biznesową, a także zaawansowane funkcje diagnozowania służące do pogłębionego badania problemu.

Rysunek 4. Strona z informacjami o anomalii

• Started at 11/28/11 6:30 AM, no end date.

Suspects:

- obadb (Node/Infrastructure)
Suspectible due to abnormal metric 'CPU Used Percentage'.
[show available run-books...](#)
- Stock Trader Host (Node/Infrastructure)
Suspectible due to abnormal metric 'CPU Used Percentage'.
[show available run-books...](#)

Additional Information:

- Advantage Banking (BusinessApplication/application_and_services)
Abnormal metric: CPU Utilization
[Run Books](#)

Business Impact:
Status of relevant SLA as of 11/28/11 10:15 AM:

- OLA - Failed
[SLM Report](#)

1 applications/services that might be affected:

- Advantage Banking
89 users out of 107 are experiencing problems as of 11/28/11 10:15 AM
[RUM Report](#)

4 locations are affected:

- New York
- London
- Paris
- Amsterdam

Similarities:

- [11/8/11 12:20 PM](#) Similarity score: 91%
- [11/8/11 7:50 PM](#) Similarity score: 78%

Note:The details are not yet final since the information is still being gathered. Try to reinvoke later for final results.

Close Investigate Further Copy to Clipboard Help

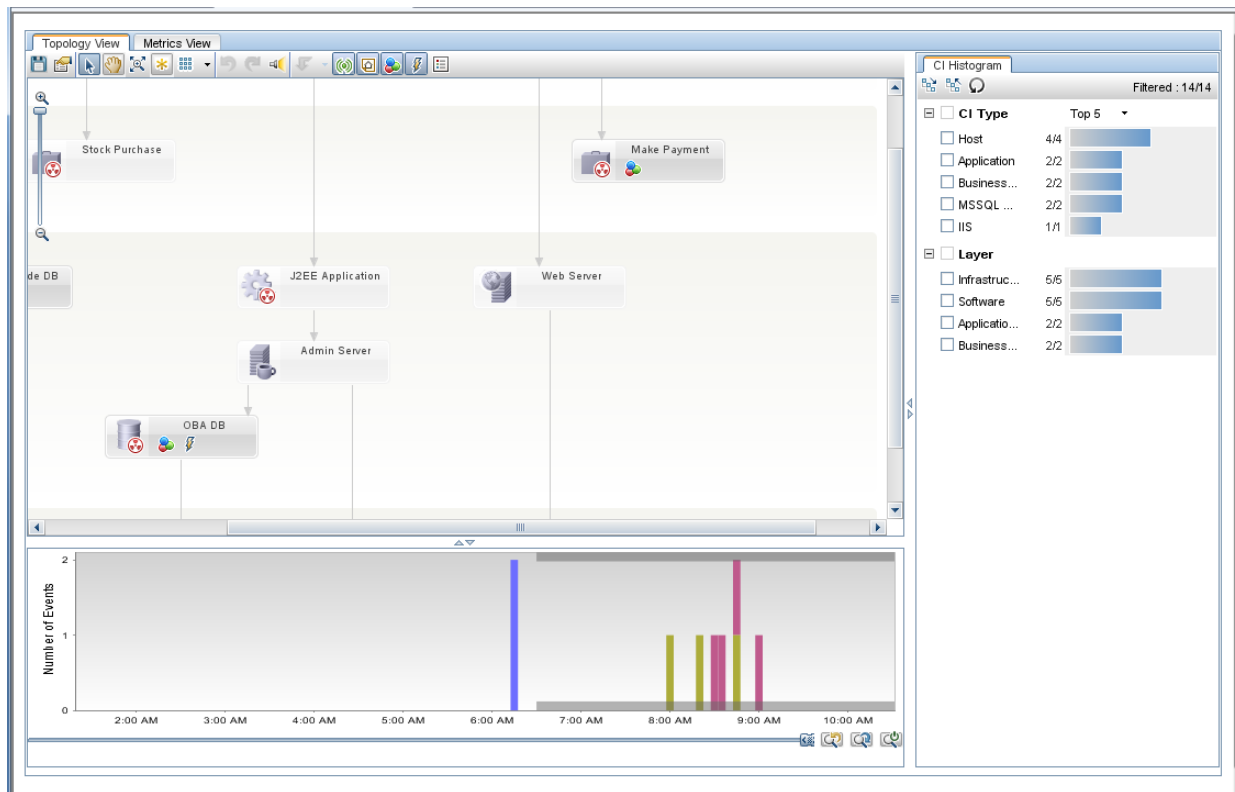
W górnej części rysunku 4 „Strona z informacjami o anomalii” można znaleźć „listę podejrzanych”. „Podejrzani” to elementy konfiguracji (aplikacje, transakcje, elementy infrastruktury), które zostały znalezione przez produkt SHA jako możliwa przyczyna anomalii. Podejrzane mogą być elementy konfiguracji, których metryki przekroczyły poziom odniesienia, wzorce anomalii, które zostały wcześniej zidentyfikowane przez użytkownika jako odbiegające od normy, oraz elementy konfiguracji, które nie przeszły weryfikacji za pomocą dostarczonego przez użytkownika narzędzia do weryfikacji.

Strona z informacjami przedstawia również wpływ anomalii na działalność biznesową, pokazując umowy dotyczące poziomu świadczonych usług, które zostały naruszone z powodu anomalii, usługi i aplikacje, których dotyczy problem, oraz analizę lokalizacji, na które wpłynął problem. Rozwiązanie SHA umożliwia także generowanie odpowiednich raportów mających na celu pogłębienie i poszerzenie wiedzy o problemie. Podobna sekcja anomalii jest generowana przy użyciu technologii Anomaly DNA. Zawiera ona listę podobnych wzorców oraz dodatkowe informacje na temat sposobu ich obsługi, dzięki czemu daje większą pewność co do wystąpienia problemu.

Rozwiązanie SHA oferuje narzędzie do badania i diagnozowania problemów, za pomocą którego można uzyskać bardziej szczegółowe informacje o anomalii oraz wyodrębnić możliwą główną przyczynę problemu w interfejsie Subject Matter Expert User Interface (SME UI). Narzędzie do badania anomalii umożliwia „podróżowanie w czasie” i zawiera szczegółowy widok kolejności zdarzeń, które doprowadziły do wystąpienia problemu, co zostało odzwierciedlone w topologii aplikacji.

Poniższy rysunek przedstawia przykład anomalii i jej kolejność zdarzeń w czasie.

Rysunek 5. Interfejs SME UI przedstawiający topologię anomalii



W dolnej części ekranu widoczne są zdarzenia, które wystąpiły w systemie i zostały przechwycone przez rozwiązanie SHA przed wystąpieniem anomalii i w trakcie jej trwania.

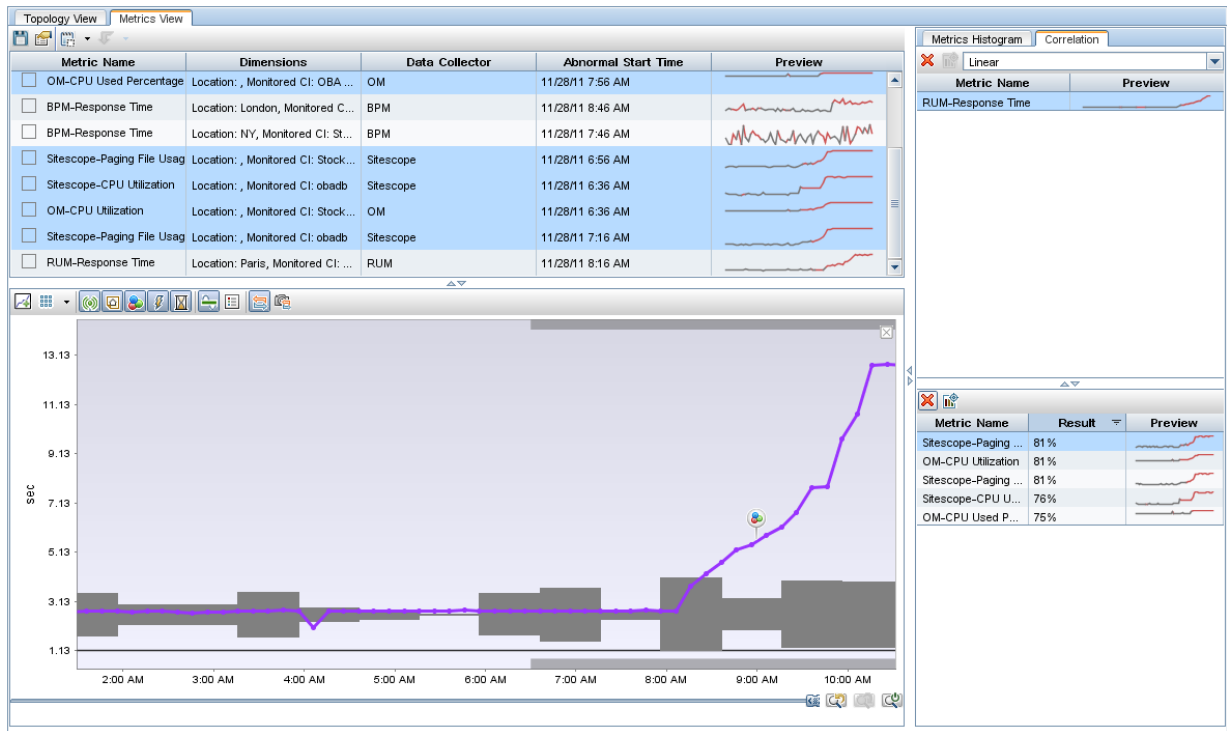
- O godzinie 6:15 rozwiązanie SHA zarejestrowało wykrycie zmiany w systemie.
- O godzinie 6:30 rozwiązanie SHA wyzwoлиło anomalię. Oznacza to, że jakieś metryki odbiegające od normy, które przekroczyły poziom odniesienia, zostały wykryte, **zanim** wykryły je rozwiązania SiteScope i OM monitorujące system. W tym momencie rozwiązanie SHA **już wyzwoлиło zdarzenie, które zostało wysłane do pracowników operacyjnych**.
- W godzinach 8:00 – 8:20 rozwiązania SiteScope i OM wyzwoлиły zdarzenia na podstawie dużego wykorzystania zasobów procesora. Przyczyna, dla której rozwiązania SiteScope i OM wykryły problem **później niż rozwiązanie SHA**, leży w tym, że ich wartości progowe zostały ustawione wyżej niż dynamiczny poziom odniesienia w rozwiązaniu SHA, aby ograniczyć liczbę niegroźnych i fałszywych alarmów.
- O godzinie 8:30 pierwszy rzeczywisty użytkownik odczuł problem z wydajnością i otworzył zdarzenie.

Jak widać, rozwiązanie SHA wykryło problem i ostrzegło o nim **dwie godziny przed** zgłoszeniem skargi przez jakiegokolwiek użytkownika, powiadamiając z awansu pracowników operacyjnych i umożliwiając im obsłużenie i rozwiązanie problemu.

Rozwiązanie SHA oferuje zaawansowane narzędzie do korelowania i wyszukiwania metryk, które mogą być główną przyczyną problemu w systemie.

Poniższy rysunek przedstawia widok metryk SHA będący częścią interfejsu SME UI.

Rysunek 6. Interfejs SME UI w widoku metryk



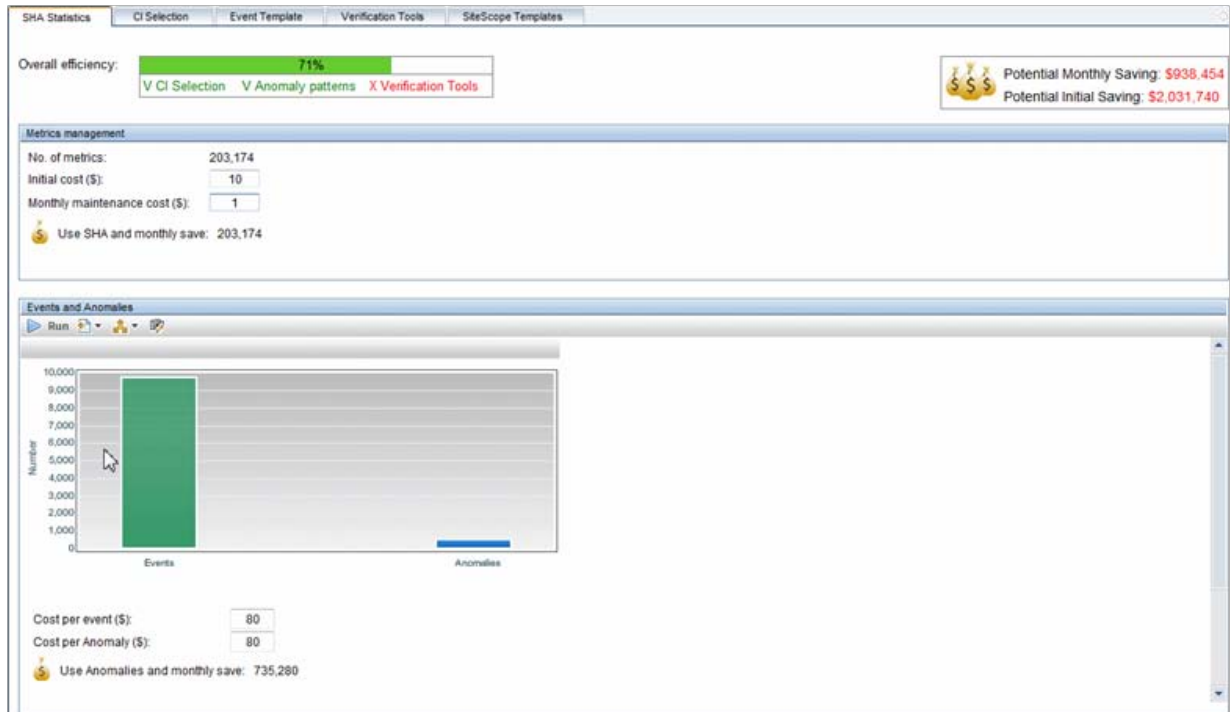
Widok metryk umożliwia wyświetlenie podglądu metryk aplikacji, które zostały przechwycone w ramach czasowych występowania anomalii w otoczeniu ich poziomu odniesienia. Pozwala także uzyskać informacje na temat metryk, które mogą być główną przyczyną problemu, przez skorelowanie ich z innymi metrykami związanymi z tą samą usługą za pomocą zaawansowanych algorytmów statystycznych.

W tym przykładzie użytkownik postanowił skorelować metrykę programu Real User Monitor (RUM) ze wszystkimi pozostałymi. Przyczyną, dla której została wybrana ta metryka, jest fakt, iż najlepiej reprezentuje ona rzeczywisty czas reakcji, z którym mają do czynienia prawdziwi użytkownicy podczas korzystania z aplikacji. Pozostałe metryki dotyczą składników infrastruktury i oprogramowania pośredniczącego, a w widoku metryk dostępny jest mechanizm „wskaz i kliknij” umożliwiający przedstawienie korelacji między nimi a długim czasem reakcji. Najwyższą wartość korelacji (81 procent) uzyskała metryka „Sitescope_paging File Usage”, która jako najbardziej prawdopodobną główną przyczynę wskazuje niewystarczający przydział pamięci.

Zwrot z inwestycji

Rozwiązanie SHA oblicza zwrot z inwestycji (ROI) przy użyciu informacji zgromadzonych ze środowiska wdrażania. W sekcji zarządzania metrykami zwrot z inwestycji oceniany jest na podstawie zmniejszenia nakładu prac administracyjnych związanych z określeniem i utrzymywaniem wartości progowych dzięki zastosowaniu samodzielnie uczących się dynamicznych wartości progowych udostępnianych przez rozwiązanie SHA. W sekcji zdarzeń i anomalii zwrot z inwestycji oceniany jest z punktu widzenia perspektywy zmniejszenia liczby zdarzeń przez porównanie bieżącego strumienia zdarzeń rozwiązania OMi ze zdarzeniami anomalii generowanymi przez rozwiązanie SHA. Te informacje w połączeniu stanowią o ogólnej skuteczności.

Rysunek 7. Widok zwrotu z inwestycji w rozwiązaniu SHA



Podsumowanie

SHA to przyszłościowe rozwiązanie firmy HP z dziedziny analizy prognostycznej w czasie wykonywania, które umożliwia przewidywanie problemów jeszcze przed ich wystąpieniem, analizując odbiegające od normy działanie usługi i alarmując menedżerów działów informatycznych o rzeczywistym obniżeniu jakości usługi, zanim problem zdąży wpłynąć na działalność biznesową. Rozwiązanie SHA zapewnia ścisłą integrację z rozwiązaniami HP BSM w celu korygowania zdarzeń i skracania średniego czasu naprawy (MTTR).

Ponadto rozwiązanie SHA jest łatwe w użyciu, wymaga minimalnych nakładów na konfigurację i ustawienia oraz ma niewielką krzywą uczenia się. Dzięki rozwiązaniu SHA nie trzeba dłużej utrzymywać wartości progowych monitorowania, ponieważ produkt przez cały czas uczy się zachowania aplikacji i odpowiednio je dostosowuje. Ponieważ w systemie występuje mniejsza liczba zdarzeń, każde z nich reprezentuje rzeczywisty problem, a produkt pozwala skupić się na głównej przyczynie, skraca się średni czas naprawy (MTTR) aplikacji. Produkt SHA jest oparty na dynamicznym rozwiązaniu HP RISM, dlatego pomaga w wykrywaniu potencjalnych problemów związanych z topologią i usługami oraz rozwiązywaniu ich, zanim jeszcze napotkają je użytkownicy końcowi.

Rozwiązanie HP SHA to nowa era w dziedzinie analizowania infrastruktury informatycznej. Więcej informacji można uzyskać na stronie www.hp.com/go/sha.



Get connected

www.hp.com/go/getconnected

Current HP driver, support, and security alerts
delivered directly to your desktop

© Copyright 2011 Hewlett-Packard Development Company, LP. Informacje zawarte w tym dokumencie mogą ulec zmianie bez powiadomienia. Gwarancje na produkty i usługi firmy HP są określone w wyraźnych warunkach gwarancji towarzyszących produktom i usługom. Żadne informacje przedstawione w niniejszym dokumencie nie powinny być interpretowane jako dodatkowa gwarancja. Firma Hewlett-Packard Company nie może być pociągana do odpowiedzialności za błędy techniczne i edycyjne, oraz za informacje pominięte w tym dokumencie.

4AA3-8672PLE, utworzono w grudniu 2011 r.

