HP Service Health Analyzer: Dekódování DNA potíží s výkonností IT

Technický dokument

Obsah

Úvod

Zajištění úplného přehledu o zdraví podnikových služeb, které můžete přizpůsobit a dokonce zajistit jejich přežití, není v dnešním cloudovém a virtualizovaném prostředí IT pouze „elegantním doplňkem“. Je to nezbytnost. Správa dynamické infrastruktury a aplikací obnáší více než jen reakce na potíže podnikových služeb nebo ruční aktualizace statických prahových hodnot, jejichž nastavení je problematické a správa náročná.

V dnešním světě potřebujete pokročilé upozorňování na problémy, abyste je mohli vyřešit dříve, než se projeví jejich dopad na podnik. Potřebujete lepší přehled o korelaci aplikací a podnikových služeb s dynamickou infrastrukturou, abyste mohli sledovat anomálie v celém rozsahu sektoru IT včetně sítě, serverů, programového vybavení, aplikací a obchodních procesů. Potřebujete snazší způsob určení přípustných mezí jako základ pro zjišťování událostí s možným dopadem na podnikovou činnost. Potřebujete automatizaci k uplatnění znalostí z minulých událostí, které lze využít k účinnějšímu řešení nových událostí a také k eliminaci vedlejších problémů, aby se sektor IT mohl zaměřit výhradně na události s dopadem na podnikovou činnost.

Organizace IT mají metody shromažď'ování ohromného množství dat, avšak doposud chyběla sada analytických nástrojů a automatická inteligence k nalezení korelace mezi těmito různorodými metrikami z pohledu jak aplikací, tak topologie, s cílem pomoci těmto organizacím předvídat a předpokládat potenciální hrozící problémy. Manažeři v oblasti IT vstupují do světa prediktivní analýzy, jednoho z nejvýznamnějších trendů podnikové inteligence v roce 2011, který jim pomůže zlepšit provozuschopnost a výkonnost služeb, a tím zvýšit výnosy z podnikové činnosti a snížit náklady na údržbu a podporu.

HP Service Health Analyzer (SHA) je prediktivní analytický nástroj založený na dynamickém modelu služeb v reálném čase, který umožňuje porozumět vztahu mezi abnormalitami metrik a aplikacemi a jejich základní infrastrukturou.

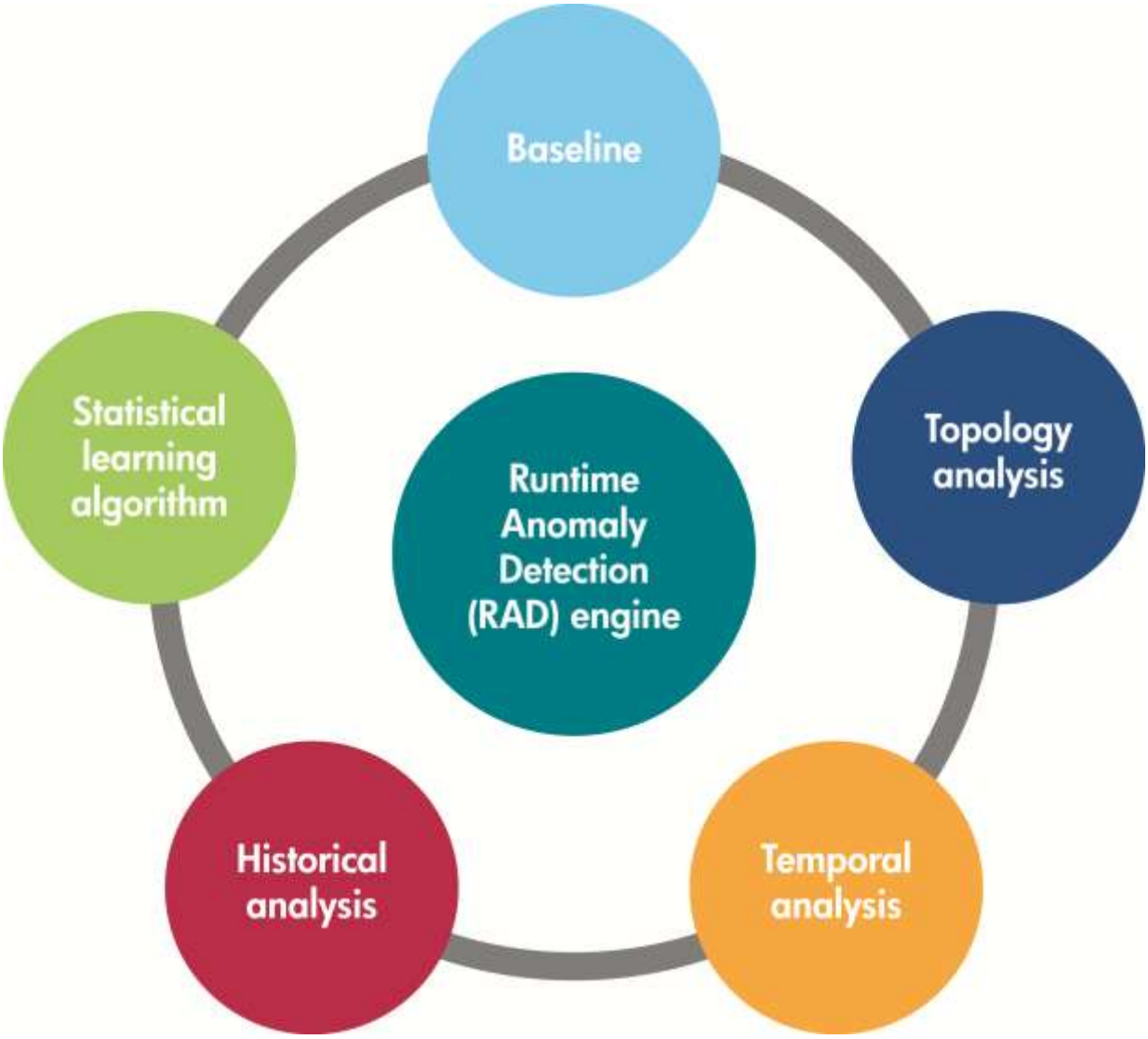
Jedinečný přístup společnosti HP – nástroj HP SHA postavený na modelu HP Run-time Service Model

Monitorovací systémy informují o naměřených hodnotách a událostech ze všech vrstev sektoru IT – hardwaru, síťových OS, programového vybavení, aplikací, podnikových služeb a procesů. Databáze CMDB (Configuration Management Database) poskytují model, který všechny tyto odlišné součásti propojuje. Avšak při neustále se měnícím charakteru systémů IT je nutné databáze CMDB neustále aktualizovat, jako je tomu v případě modulu HP Run-time Service Model (RtSM). Kombinace monitorování a databází CMDB v reálném čase poskytuje veškerá data nutná ke splnění výše uvedených nároků. K získání využitelných informací je však nutné všechna data transformovat. Nástroj HP SHA používá pokročilé algoritmy, které spojují několik disciplín, topologii, analýzu dat, teorii grafů a statistiku v modulu Run-time Anomaly Detection (RAD).

Řešením společnosti HP pro zastaralý model služeb je modul RtSM. Modul RtSM provádí synchronizaci s databází HP UCMDB s cílem využít modelování služeb v „externí“ databázi Universal Configuration Management Database (UCMDB). Poté modul RtSM využívá kolektory dat z portfolia HP Business Service Management (BSM), které slouží k monitorování výkonnosti, dostupnosti, závad a topologie a sdílení topologie „v reálném čase“, aby měl model RtSM k dispozici co nejaktuálnější přehled o topologii a vztazích. Modul RtSM tvoří jádro nástroje SHA.

Další informace o tom, jak modul RtSM používá databáze UCMDB, naleznete v části „Průvodce osvědčenými postupy pro modul RtSM“.

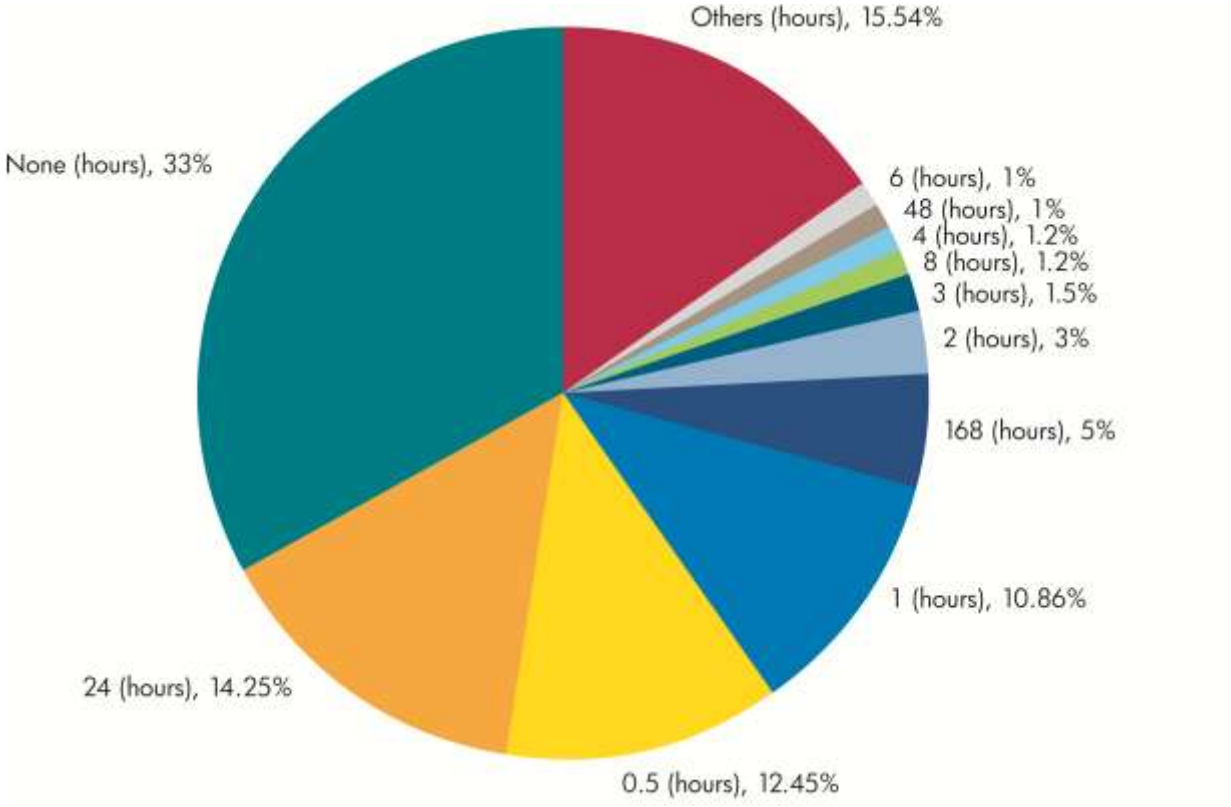
Obrázek 1. Šablona řešení



Obrázek 1 znázorňuje součásti nástroje SHA, které považujeme za nezbytné k přesnému řešení a dekódování potíží s výkonností IT. Jednotlivé součásti a související požadavky jsou představeny dále.

Stanovení základní úrovně je první součástí, která zohlední všechny metriky získané monitorovacími systémy a zjistí normální chování. Odchylky od normálního chování podle metrik slouží jako první krok při detekci, predikci a dekódování potíží s výkonností. Přesné zjištění normálního chování metrik je však náročný úkol. Faktory jako sezónní chování, trendy a změny způsobené nepřetržitým vývojem systému IT vyžadují algoritmus učení, který zohlední adaptabilitu základní úrovně a možný vliv těchto faktorů. Obrázek 2 znázorňuje rozdělení sezóny pro více než 17 000 metrik výkonnosti získaných ze skutečného systému IT. Jedná se o kombinaci monitorování systému, aplikací a uživatelské úrovně. Je patrné, že více než dvě třetiny metrik vykazují určité sezónní chování, a to v rámci rozsahu několika sezón, nikoli pouze v rámci běžně předpokládaného denního či týdenního členění. Algoritmus základní úrovně musí v první řadě přesně posoudit sezónu – vykazuje-li metrika například sezónní interval 5 hodin a algoritmus základní úrovně tuto sezónu ignoruje nebo používá nesprávnou předem danou délku sezóny (např. 24 hodin), povede
to ke zjištění nevhodné základní úrovně. Základní úroveň bude příliš citlivá a povede k detekci příliš mnoha falešných odchylek od normálu, které budou ve skutečnosti normální, nebo bude naopak příliš necitlivá a nezjistí odchylky od normálního chování, které budou skutečné.

Obrázek 2. Rozdělení sezónního chování mezi více než 17 000 metrikami získanými z prostředí IT



Podobně platí, že je pro určení základní úrovně důležitý odhad trendů a přizpůsobení změnám.

Porozumění normálnímu chování jednotlivých metrik je důležité, není však dostačující k detekci a predikci skutečných problémů. Některé odchylky od základní úrovně nebudou ze své podstaty souviset se žádným problémem (jedná se o malou část); v rozsáhlém prostředí IT s několika miliony metrik může i tato malá část vést k mnoha falešným upozorněním, pokud budou samostatně považovány za problém. Kromě toho platí, že problémy se v prostředí obvykle neprojevují prostřednictvím pouze jedné metriky.

Temporální analýza: Jedná se o jeden z rozšířených přístupů, který slučuje metriky do jedné anomálie. Metody temporální analýzy zahrnují korelace mezi metrikami, kdy jsou metriky seskupeny na základě podobnosti měření v průběhu času, či temporální analýzu/predikci s více proměnnými, která slučuje více metrik pomocí obvykle lineárního matematického modelu pro více proměnných, např. regrese více proměnných, neurálních nebo bayesovských modelů.

Tyto metody jsou účinné, avšak mají svá omezení. Za prvé, neumožňují vhodné škálování podle počtu metrik. Za druhé, z důvodu svého statistického charakteru mohou zjistit zavádějící korelace, pokud zpracovávají velmi vysoký počet metrik, mezi nimiž neexistuje skutečný vztah; pravděpodobnost zjištění takovýchto nesprávných korelací se zvyšuje s počtem metrik.

Analýza topologie: Pomáhá temporálním metodám překonat omezení v kontextu prostředí. Zejména v prostředí IT je nutné omezit analyzovanou sadu metrik na logickou sadu souvisejících metrik. Pokud procesory dvou zcela nezávislých serverů dosáhnou ve stejný čas vysokých hodnot, nelze to považovat za korelaci, přestože to tak statisticky může vypadat. Tento kontext je dán topologií systémů IT prostřednictvím databází CMDB. Databáze CMDB je v podstatě graf, který modeluje vztahy mezi všemi součástmi, z nichž se systémy IT skládají – fyzická zařízení, programové vybavení, software, aplikace, obchodní služby a procesy. K získání kontextových informací v rámci databáze CMDB je proto nutná analýza topologie ve formě pokročilých grafických algoritmů, která pomáhá detekovat skutečné problémy a korelace mezi metrikami, přičemž filtruje rušivá data.

Detekce skutečného problému tedy vyžaduje detekci vzorců odchylek od normality u mnoha metrik v určitém časovém rozsahu, které jsou filtrovány podle topologie. To vede ke statistickým metodám učení, které analyzují temporální a topologická data.

Historická analýza: Kromě detekce a predikce problémů umožňuje topologie zjištění rozsahu problému a odlišení základních příčin od příznaků; oba tyto kroky jsou pro rychlé řešení problémů důležité. Když je problém detekován a analyzován, vzorec jeho DNA je dekódován a lze jej uložit ve znalostní databázi. Využití znalostní databáze vyžaduje algoritmy pro provádění historické analýzy. Patří sem algoritmy pro nalezení shod a porovnání různých vzorců DNA problémů, vytváření clusterů a techniky klasifikace. Použití znalostní databáze a algoritmů přispívá k rychlejšímu řešení potíží a automatickému nalezení základních příčin i řešení nových problémů.

Modul RAD: Je definován jako kompletní sada algoritmů. Algoritmy v rámci modulu RAD podléhají 10 samostatným patentovým aplikacím. Výstupem modulu RAD je klíčový ukazatel výkonnosti (KPI) na ovládacím panelu HP BSM, který odesílá událost do podsystému událostí BSM – HP Operations Manager i (OMi). Událost z nástroje SHA obsahuje množství kontextových informací získaných modulem RAD, mezi které patří hlavní potenciální příčiny, informace o umístění, informace o dopadu na činnost podniku, seznam položek konfigurace (CI), které jsou součástí anomálie, a další související informace o anomálii. Tyto informace pomáhají zákazníkům rychle identifikovat a vyřešit událost tak, aby nedošlo k ovlivnění činnosti podniku.

HP SHA – prediktivní analýza v průběhu činnosti

V rámci nástroje SHA jsme vyvinuli statistické algoritmy učení kombinované s grafickými algoritmy za účelem analýzy celého spektra dat shromážděných pomocí systémů BSM:

- data monitorování (syntetických i skutečných uživatelů),
- události,
- změny,
- topologie z modulu RtSM.

Tyto algoritmy přesně detekují anomálie, dekódují jejich strukturu DNA, zjišťují dopad na podnikovou činnost a porovnávají je s dříve detekovanými anomáliemi uloženými v databázi Anomaly DNA Knowledgebase.

Nástroj SHA lze popsat následujícími kroky:

- **Učení chování metrik**

  Nezbytným prvním krokem je zjištění normálního chování, rovněž označované jako stanovení základní úrovně, metrik shromážděných ze všech úrovní služby (systému, programového vybavení, aplikací aj.). Odstraňuje nutnost nastavení statických prahových hodnot a umožňuje včasnou detekci odchylek od normálních hodnot. Klíčové stránky našich algoritmů:
  - **Automatické** učení sezónních chování metrik a jejich trendů
  - **Přizpůsobení** změnám chování v průběhu času – nutnost ve virtualizovaných prostředích
  - **Bez konfigurace** – nastavení a správa mezních hodnot nevyžadují žádné administrativní úkony

- **Technologie Anomaly DNA – detekce**

  Když začne v rámci služby IT vznikat holistický problém, dochází k odchylkám od normálního chování u řady metrik a součástí, které s touto službou souvisejí. Vyskytují se však i neustálé momentální odchylky od normality v případě řady součástí, které nepředstavují žádný významný problém. Výběr významných problémů a zjištění DNA je úkolem pro systém detekce anomálií. Náš algoritmus pro detekci DNA anomálií toho dosahuje pomocí jedinečného statistického algoritmu, který kombinuje tři druhy informací nutných k dosažení přesné detekce:
  - **Topologické**: logická spojení mezi monitory a monitorovanými součástmi.
  - **Temporální informace**: doba trvání a časová korelace monitorů, které jsou v nenormálním stavu.
  - **Informace o statistické důvěryhodnosti**: pravděpodobnost, že je monitor skutečně v nenormálním stavu, určená na základě základní úrovně stanovené v průběhu času.

Klíčové silné stránky našeho algoritmu detekce anomálií:

- **Redukce nepřehlednosti**: Poskytuje automatickou metodu seskupení metrik, které porušily základní hodnoty, pomocí temporálních i topologických informací. Tím dochází ke snížení počtu událostí s porušenou základní úrovní, které vyžadují pozornost obsluhy, bez nutnosti nastavení pravidel.
- **Snížení počtu událostí**: Algoritmy nástroje SHA slučují několik nenormálních metrik do jediné události, čímž snižují celkový počet událostí předložených obsluze. Vstupní úroveň tohoto typu událostí představuje porušení dynamických mezních hodnot u několika metrik. Nástroj SHA poté provede korelaci těchto metrik podle času a topologie a vygeneruje jedinou událost, která obsluze umožní soustředit se na skutečný problém.
- **Redukce falešných poplachů**: Snižuje počet falešných výstrah vypočítáním významnosti anomálie v systému pomocí statistického algoritmu. K potlačení události anomálie budou také použity známé anomálie, které byly v minulosti označeny jako rušivé.

- **Technologie Anomaly DNA – dekódování**

  Dalším krokem po detekci anomálie a její struktury je dekódování její DNA. Dekódování DNA anomálie má podobu analýzy a zařazení na základě topologie (CI a jejich topologické struktury), metrik a dalších informací. Konkrétní cíle dekódování:
  - Oddělení podezřelých příčin, které přináší využitelné informace. Určení dopadu na podnikovou činnost pomocí podnikových informací: objemu uživatelů, smluv o úrovni služeb (SLA) a postižených geografických oblastí. To umožňuje určení priority anomálie na základě dopadu.
  - Zjištění souvisejících změn, které mohly ovlivnit chování systému

- **Technologie Anomaly DNA – porovnání**

  Po dekódování struktury DNA anomálie probíhá porovnání aktuální anomálie s minulými anomáliemi. K porovnání je použit jedinečný algoritmus podobnosti grafů, který srovnává abstraktní struktury anomálií, čímž umožňuje nalezení shod mezi anomáliemi, které byly detekovány u různých služeb s podobnou architekturou. Výhody našeho porovnání:
  - Umožňuje opakované využití řešení nalezených u minulých událostí.
  - Přiřazuje anomálie ke známým potížím, které dosud nebyly vyřešeny, čímž omezuje nutnost opakovaného zjišťování.
  - Snižuje počet falešných poplachů, pokud byla podobná anomálie v minulosti klasifikována jako rušivá struktura DNA, například v případě anomálií způsobených běžnými postupy údržby či servisu.

- **Znalostní databáze Anomaly DNA Knowledgebase**

  Při shromažďování informací o minulých anomáliích a jejich řešeních dochází k vytvoření znalostní databáze. Pomocí pokročilých metod dolování dat jsou generovány a analyzovány vztahy mezi všemi anomáliemi a je vytvářena mapa celé databáze Anomaly DNA Knowledgebase. Náš algoritmus porovnávání DNA anomálií definuje požadovaný prostor metrik pro metody dolování dat jako clustering a klasifikace. Jejich použití přináší následující výhody:
  - Proaktivní řešení potíží – zjištění opakujících se problémů prostřednictvím klasifikace DNA anomálií do typů problémů a řešení, které zkracuje dobu diagnostiky a řešení u těchto typů v budoucnosti
  - Využití znalostí získaných z různých služeb, které vykazují podobné chování

Možnosti produktu

Nástroj HP SHA postavený na modulu HP RtSM analyzuje historické normy a trendy aplikací a infrastruktury a porovnává tato data s metrikou výkonu v reálném čase. Použití modelu služeb v době provozu je pro vaše dynamické prostředí klíčové a přináší následující možnosti:

- Korelace anomálií se změnami topologie a minulými problémy
- Pochopení dopadu každého problému na firmu a určení priorit pro řešení
- Zjištění podezřelých příčin problému a využití těchto znalostí při prevenci podobných problémů v budoucnosti

Nástroj SHA se automaticky učí dynamické mezní hodnoty ve vašem prostředí, nemusíte tedy vynakládat úsilí na nastavení a správu statických mezí. Nástroj SHA zpracovává metriky z následujících zdrojů dat BSM:

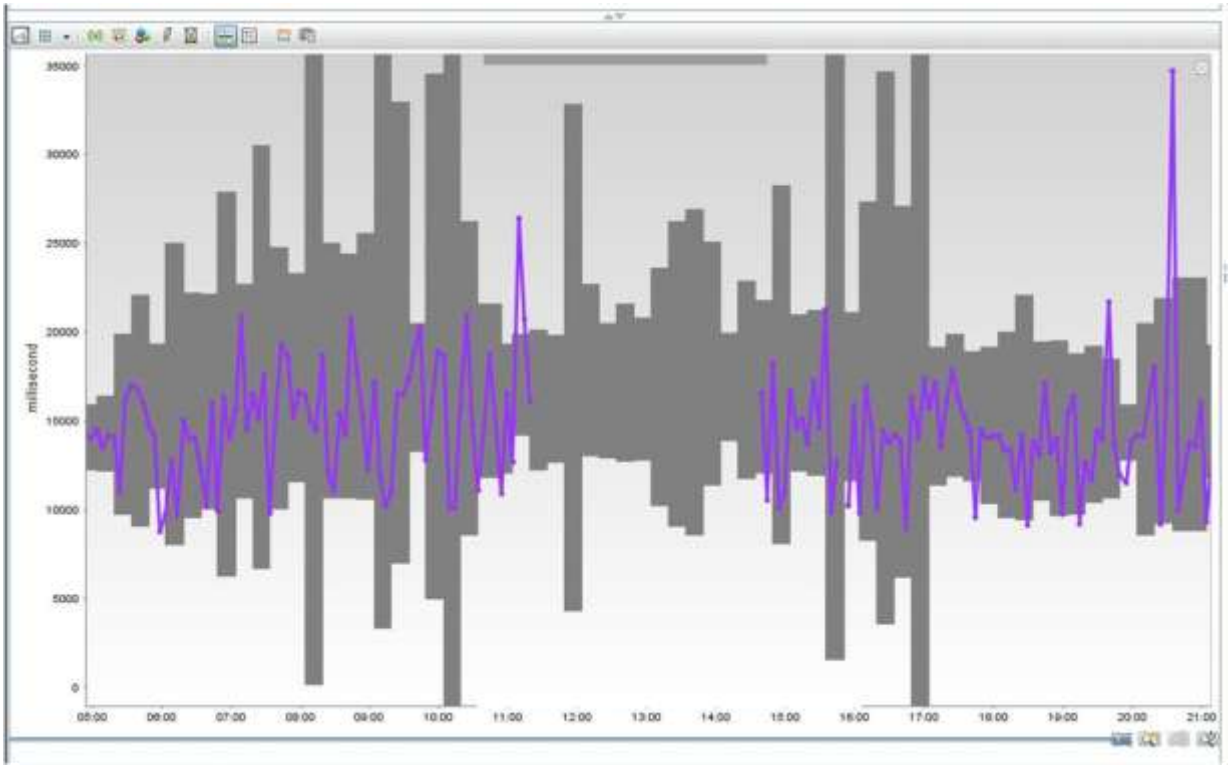
- HP Business Process Monitor,
- HP Diagnostics,
- HP Network Node Manager i,
- HP Operations Manager, Performance Agent,
- HP Real User Monitor,
- HP SiteScope.

Nástroj SHA rozpoznává anomálie na základě nenormálního chování metrik týkajících se modulu RtSM, stanovuje ukazatele KPI a generuje události s kontextem, který vám pomůže rozpoznat podnikovou prioritu daného problému. Nástroj SHA také používá technologii Anomaly DNA pro analýzu struktury anomálie a porovnává ji se známými strukturami DNA jiných anomálií. Shody poskytují známé akce k řešení problémů bez dalšího zkoumání a současně jsou potlačeny shody označené jako šum. Pokud u určité služby vzniknou anomálie, můžete zjistit, na kterou smlouvu SLA a jak velký dopad tento stav bude mít. Nástroj SHA rovněž zahrnuje možnosti opravných postupů z řešení HP Closed Loop Incident Process (CLIP) a umožňuje přímou integraci se softwarem HP Operations Orchestration. Můžete například sloučit analýzu a automatizaci, a dosáhnout tak rychlejšího odstraňování problémů. Když nástroj SHA odešle událost do subsystému OMi, může obsluha provést akci předtím, než dojde k narušení služby, pomocí procesu CLIP. Toto rychlé řešení problémů zjednodušuje složitost virtualizace a cloudového prostředí.

Začněte s nulovou konfigurací a nulovou údržbou

Po instalaci produktu vyberete aplikace, které chcete monitorovat; nástroj SHA začne sbírat data a seznamovat se s chováním systému. Nástroj SHA získá data z aplikace, infrastruktury, databáze, sítě, programového vybavení a také informace o topologii z modulu RtSM a stanoví základní úroveň. Základní úroveň definuje normální chování jednotlivých metrik v průběhu času, a to včetně sezónních vlastností. Normální chování metriky může například zahrnovat velmi vytížené pondělní ráno a naopak velmi klidné páteční odpoledne.

Obrázek 3. Příklad dynamické základní úrovně v šedém pásmu se skutečnými daty metrik znázorněnými fialově



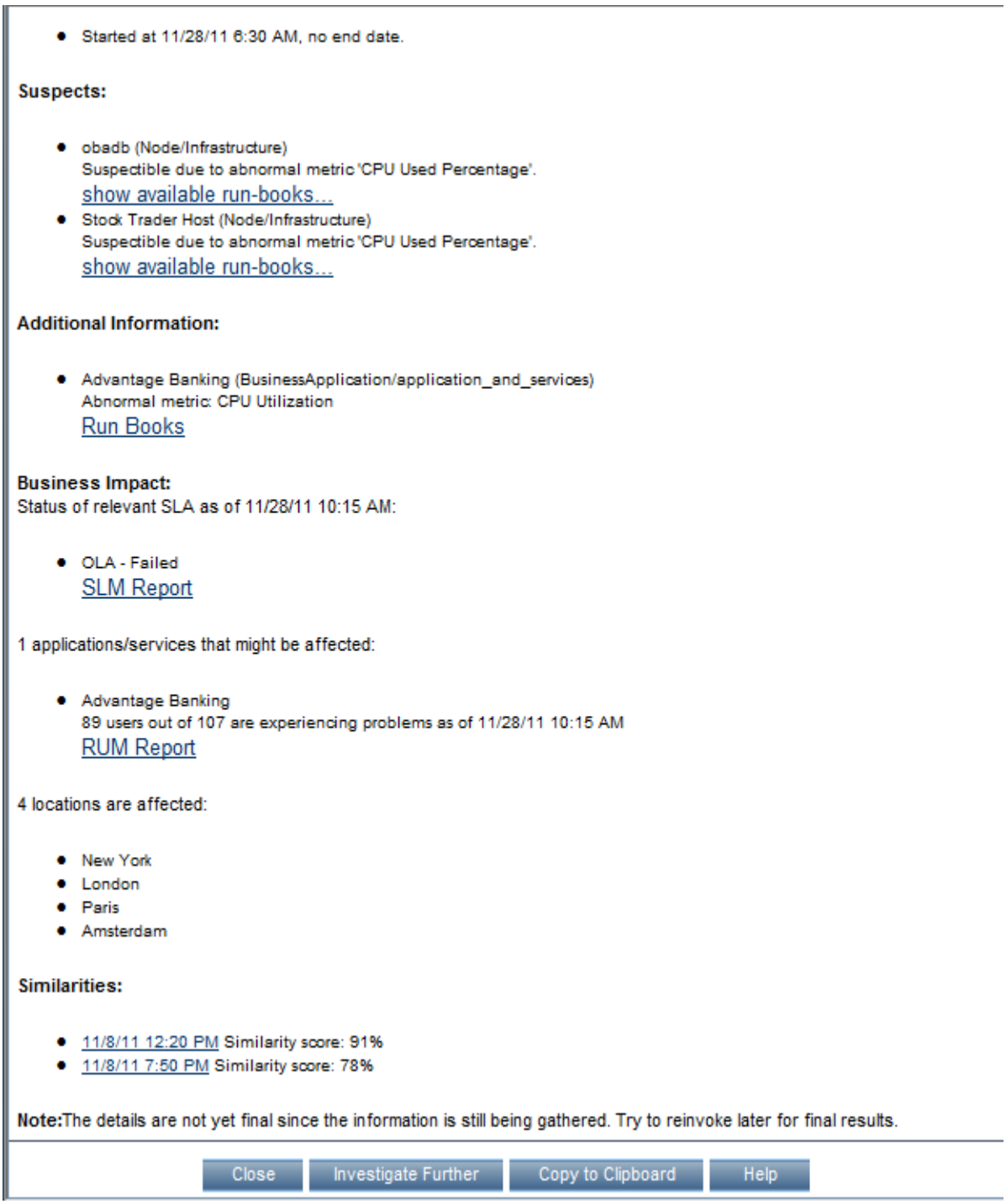
Po stanovení dynamické základní úrovně pro všechny metriky aplikací začne modul SHA RAD vyhledávat anomálie v chování aplikací. Vstupní úrovní pro modul RAD je narušení základní úrovně, což znamená, že metrika vykazuje nenormální chování. Modul RAD definuje anomálii tak, že použije všechny informace o abnormálních hodnotách metrik získané ze všech monitorovaných metrik a přiřadí je k informacím o topologii z modulu RtSM s cílem zjistit, zda došlo k několika narušením u

různých metrik, které mají dopad na stejnou službu. Je-li anomálie detekována, dojde k vygenerování události, která je odeslána do subsystému událostí. Nástroj SHA dále při zjištění anomálie automaticky zaznamená aktuální topologii položek CI, které jsou součástí události. Umožňuje to poznat stav topologie v době výskytu anomálie, což je obzvláště cenné při kontrole anomálií, ke kterým došlo přes noc nebo když v danou dobu nebyly k dispozici žádní zaměstnanci oddělení IT, kteří by mohli problémy vyřešit. Nástroj SHA také shromažďuje a předkládá zjištěné změny příslušných položek CI; tyto informace lze použít při analýze základní příčiny. Tato korelace znamená rychlejší řešení potíží a zkrácenou střední dobu do provedení opravy (MTTR).

Když nástroj SHA zjistí anomálii v chování aplikace, změní stav ukazatele KPI Predictive Health a vytvoří událost, kterou odešle do prohlížeče událostí BSM. Od tohoto bodu můžete začít zkoumat podrobnosti, izolovat problém a zjistit jeho dopad na podnikovou činnost.

Nástroj SHA obsahuje stránku s hlavními údaji o anomáliích, která uvádí všechny potřebné informace o problému a jeho dopadu na podnikovou činnost, a také pokročilé možnosti izolace pro případ, že potřebujete problém dále podrobněji zkoumat.

Obrázek 4. Stránka se základními údaji o problému



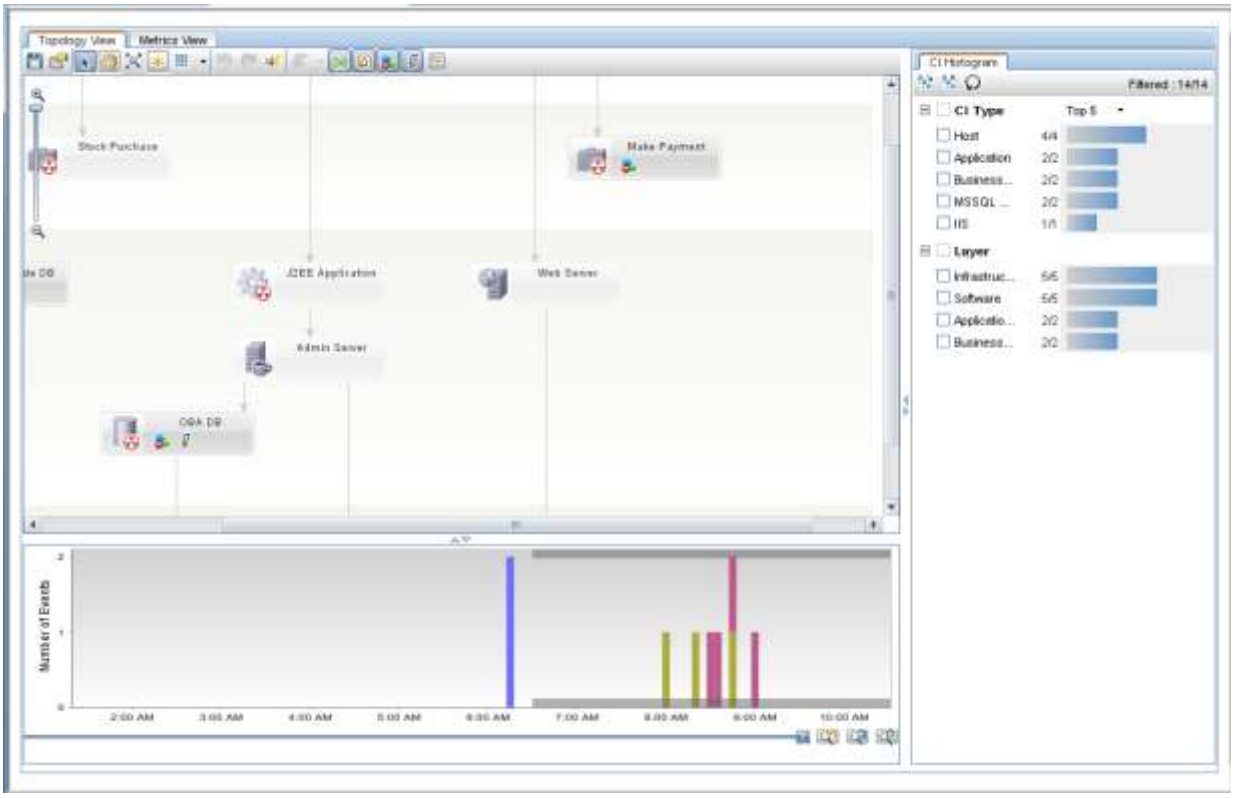
V horní části obrázku 4 „Stránka se základními údaji o problému" se nachází „seznam podezřelých příčin". Podezřelými příčinami jsou položky CI (aplikace, transakce, prvky infrastruktury), které nástroj SHA rozpoznal jako možné příčiny anomálie. Mezi podezřelé příčiny mohou patřit položky CI, u nichž metriky překročily základní úroveň, vzorce anomálií, které byly dříve uživatelem rozpoznány jako nenormální, a položky CI, které se nepodařilo ověřit pomocí vlastního uživatelského nástroje pro ověření.

Stránka se základními údaji rovněž informuje o dopadu anomálie na podnikovou činnost a uvádí, které smlouvy SLA byly z důvodu anomálie porušeny, ovlivněné služby a aplikace a přehled postižených lokalit. Nástroj SHA rovněž nabízí vytvoření odpovídajících zpráv pro analýzu a získání lepšího přehledu o problému. Podobná sekce anomálií je generována pomocí technologie Anomaly DNA, která lépe potvrzuje výskyt problému zobrazením seznamu podobných vzorců a uvádí další informace o jejich zpracování.

Nástroj SHA poskytuje nástroje ke zkoumání a izolaci problému, podrobnému rozboru anomálie a určení možné základní příčiny problému pomocí rozhraní Subject Matter Expert User Interface (SME UI). Nástroj pro zkoumání umožňuje „cestovat v čase" anomálií a získat podrobný přehled o sledu událostí, které vedly k problému, zaznamenaném v topologii aplikace.

Následující obrázek znázorňuje příklad anomálie a její průběh v čase.

Obrázek 5. Rozhraní SME UI znázorňující topologii anomálie



Dolní část obrazovky znázorňuje události v systému tak, jak k nim došlo a jak byly nástrojem SHA zaznamenány v průběhu času před anomálií a během ní.

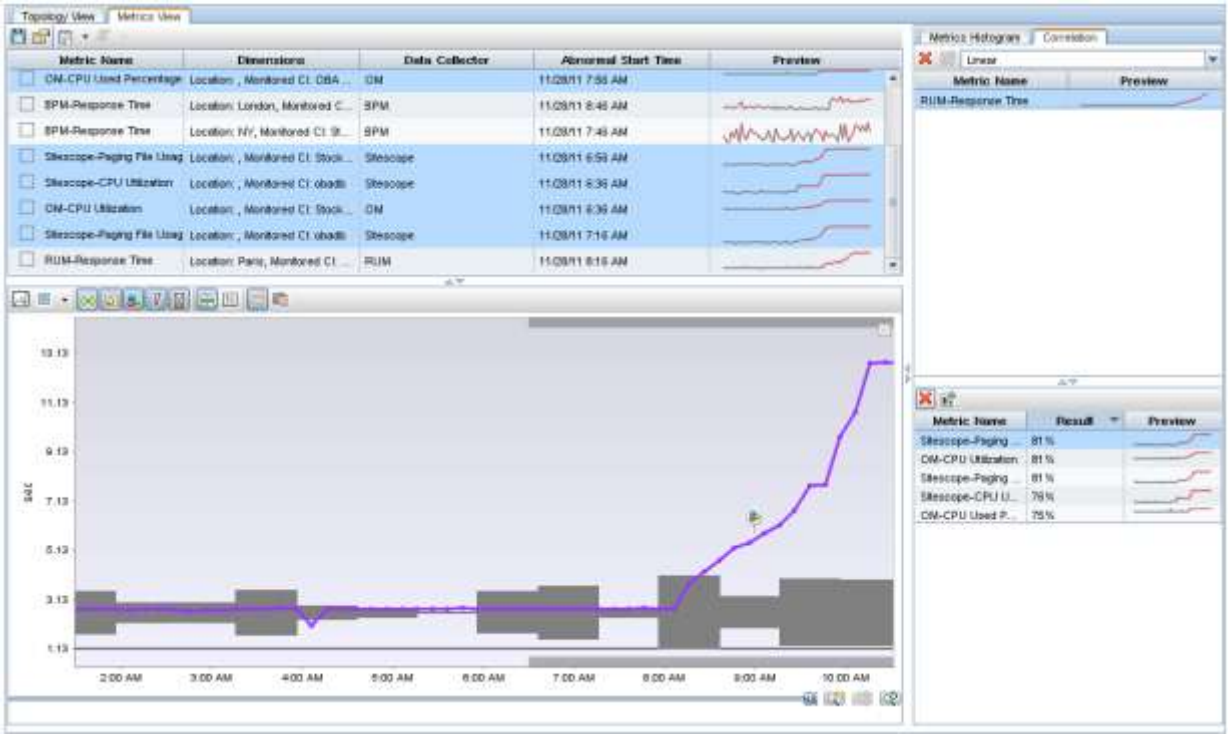
- V 6:15 zaznamenal nástroj SHA zjištění změny v systému.
- V 6:30 spustil nástroj SHA anomálii. To znamená, že detekoval několik nenormálních metrik, které překročily základní úroveň – **dříve,** než tento stav detekovaly nástroje SiteScope a OM monitorující systém. V této chvíli již nástroj SHA **vytvořil událost, která byla odeslána obsluhujícímu personálu**.
- V době mezi 8:00 – 8:20 oznámily nástroje SiteScope a OM události vysokého využití procesorů. Důvodem, proč nástroje SiteScope a OM zjistily problém **později než SHA**, je vyšší nastavení mezních hodnot, než je dynamická základní úroveň nástroje SHA – za účelem snížení rušení a falešných pozitivních upozornění.
- V 8:30 zaznamenal první uživatel problém s výkonností a otevřel incident.

Je zřejmé, že nástroj SHA zjistil problém a upozornil na něj **s dvouhodinovým předstihem** a dříve, než si začali uživatelé stěžovat, což obslužnému personálu poskytuje předčasné upozornění a čas na zpracování a vyřešení problému.

Nástroj SHA je výkonným nástrojem pro nalezení korelace a zjištění metrik, které mohou být potenciální základní příčinou problému v systému.

Následující obrázek znázorňuje zobrazení metrik nástroje SHA v rámci rozhraní SME UI.

Obrázek 6. Zobrazení metrik v rozhraní SME UI



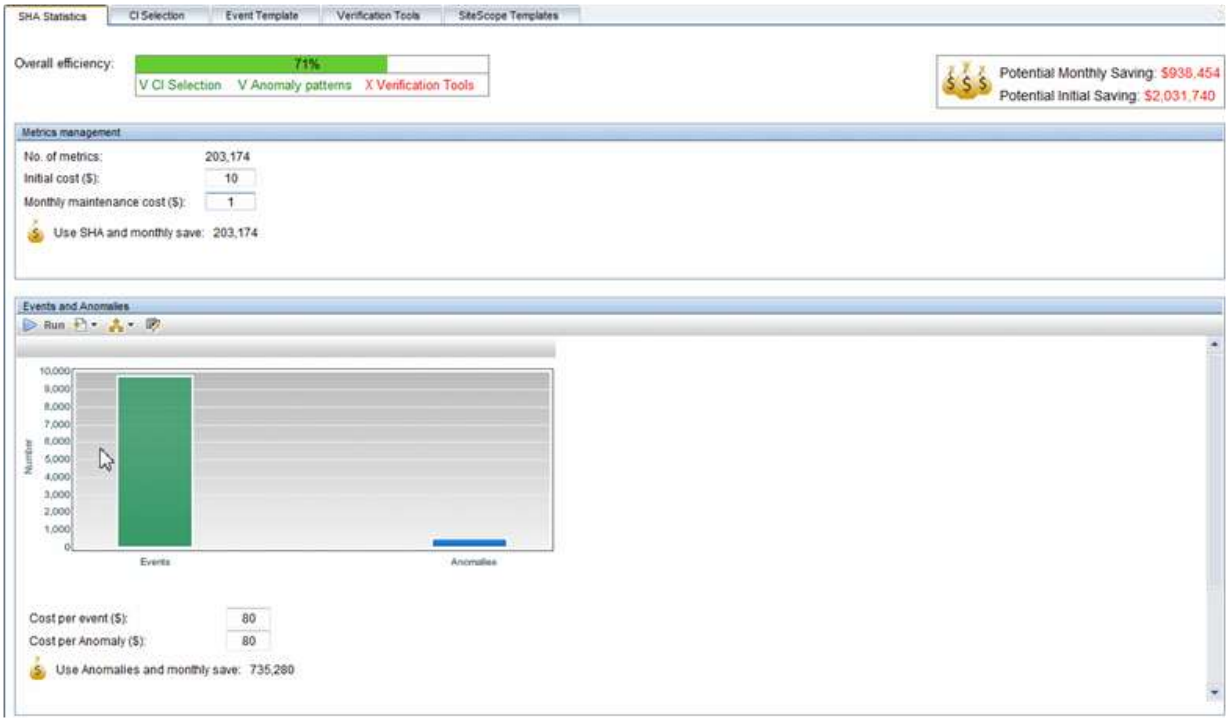
Zobrazení metrik umožňuje získat náhled metrik aplikací podle toho, jak byly zaznamenány během anomálie v „obálce" základní úrovně. Můžete zde také zjistit, která z metrik byla základní příčinou problému, nalezením vztahu s jinými metrikami, které souvisejí se stejnou službou, pomocí sofistikovaných statistických algoritmů.

V tomto příkladu se uživatel rozhodl zjistit vztah metriky Real User Monitor (RUM) s ostatními metrikami. Důvodem pro výběr této metriky je to, že vyjadřuje skutečný čas odezvy, který uživatelé zaznamenávají při použití aplikace. Zbývající metriky se týkají infrastruktury a programového vybavení, přičemž zobrazení metrik poskytuje možnost zobrazení vztahu mezi těmito metrikami a dobou odezvy pouhým výběrem a kliknutím. Metrikou s nejvyšší hodnotou korelace (81 %) je „Sitescope_paging File Usage", která signalizuje, že základní příčinou je pravděpodobně nedostatečná alokace paměti.

Návratnost investic

Nástroj SHA vypočítává návratnost investic (ROI) pomocí informací získaných z prostředí nasazení. Část pro správu metrik sleduje hodnotu ROI dosaženou snížením administrativních úkonů nastavování a správy mezních hodnot pomocí vlastního učení dynamických mezí, které nástroj SHA umožňuje. Část událostí a anomálií přistupuje k hodnotě ROI z pohledu snížení počtu událostí srovnáním stávajícího toku událostí subsystému OMi s počtem anomálií vygenerovaným nástrojem SHA. Tyto informace jsou přičteny k celkové účinnosti.

Obrázek 7. Zobrazení ROI nástroje SHA



Závěr

Nástroj SHA představuje řešení příští generace od společnosti HP pro prediktivní analýzu v době provozu, které dokáže předpokládat potíže IT dříve, než se vyskytnou, na základě analýzy nenormálního chování služeb a upozornit vedoucí pracovníky v oblasti IT na skutečný pokles úrovně služeb před tím, než bude mít problém dopad na činnost podniku. Nástroj SHA umožňuje úzkou integraci s řešeními HP BSM pro opravy událostí a zkracuje dobu MTTR.

Použití nástroje SHA je jednoduché, nástroj vyžaduje minimální konfiguraci a nastavení a lze se rychle seznámit s jeho použitím.
Při použití nástroje SHA již nebudete muset spravovat mezní hodnoty pro monitorování, protože nástroj se nepřetržitě učí chování aplikací a přizpůsobuje se odpovídajícím způsobem. Zkracuje dobu MTTR u aplikací, protože do systému odesílá nižší počet událostí, z nichž každá představuje vlastní problém, a soustředí se na základní příčinu. Protože je nástroj SHA postaven na dynamickém modulu HP RtSM, pomáhá zjistit potenciální příčiny při provozu IT v rámci topologie i služeb a vyřešit je dříve, než problém zaznamenají koncoví uživatelé.

Nástroj HP SHA představuje novou éru analytiky v oblasti IT. Další informace naleznete na adrese www.hp.com/go/sha.

4AA3-8672CSE, vytvořeno v prosinci 2011