HP Service Health Analyzer: Decodificare il DNA dei problemi di prestazioni IT.

Technical white paper

Sommario

Introduzione....2
Un approccio unico: il modello di servizio HP Run-time applicato ad HP SHA....2
L'analisi previsionale in tempo reale di HP SHA....5
Capacità del prodotto....6
Avvio rapido con zero configurazioni e zero mantenimento....7
Ritorno sull'investimento....12
Conclusione....12

Introduzione

Avere una completa visibilità sullo stato funzionale dei servizi business, capacità di adattarsi e, addirittura di sopravvivere nell'attuale mondo della virtualizzazione e del cloud non è un optional. È un obbligo. Per gestire un'infrastruttura dinamica e le applicazioni alla base dei servizi aziendali non basta reagire ai problemi quando si verificano, o gestire manualmente soglie statiche complesse da impostare e mantenere con precisione.

Per non impattare i servizi bisogna che i problemi vengano notificati in anticipo, così da poterli risolvere senza conseguenze per il business. Per questo occorre una maggiore visibilità sulle correlazioni tra le applicazioni servizi business e infrastruttura dinamica, in modo da poter tracciare le anomalie sull'intero stack IT: dalla rete ai server, dal middleware alle applicazioni, fino ai processi per le funzioni di business propriamente intesi. È necessario un modo più semplice per stabilire delle soglie accettabili a partire dalle quali verranno identificati gli eventi suscettibili di impattare l'attività. È inoltre necessaria l'automazione, per far leva su quanto appreso dagli eventi passati al fine di gestire in modo più efficiente quelli nuovi ed eliminare quelli estranei, consentendo così all'IT di concentrarsi solo sugli eventi che hanno un reale impatto sul il business.

Pur disponendo dei mezzi per raccogliere enormi quantità di dati, la mancanza di strumenti analitici e dell'intelligenza automatizzata necessaria correlare metriche applicative e topologiche diversificate, ha impedito finora alle organizzazioni IT di anticipare o prevedere potenziali problemi all'orizzonte. Oggi, invece, i responsabili IT guardano al mondo delle analisi previsionali, uno dei trend di spicco del 2011 in ambito di business intelligence, per migliorare la continuità e le prestazioni dei servizi così da rafforzare la redditività delle attività e ridurre i costi di gestione e supporto.

HP Service Health Analyzer (SHA) è uno strumento di analisi previsionale basato su un modello di servizio dinamico, in tempo reale, che consente di comprendere le relazioni tra le metriche anomale, le applicazioni e infrastruttura sottostante.

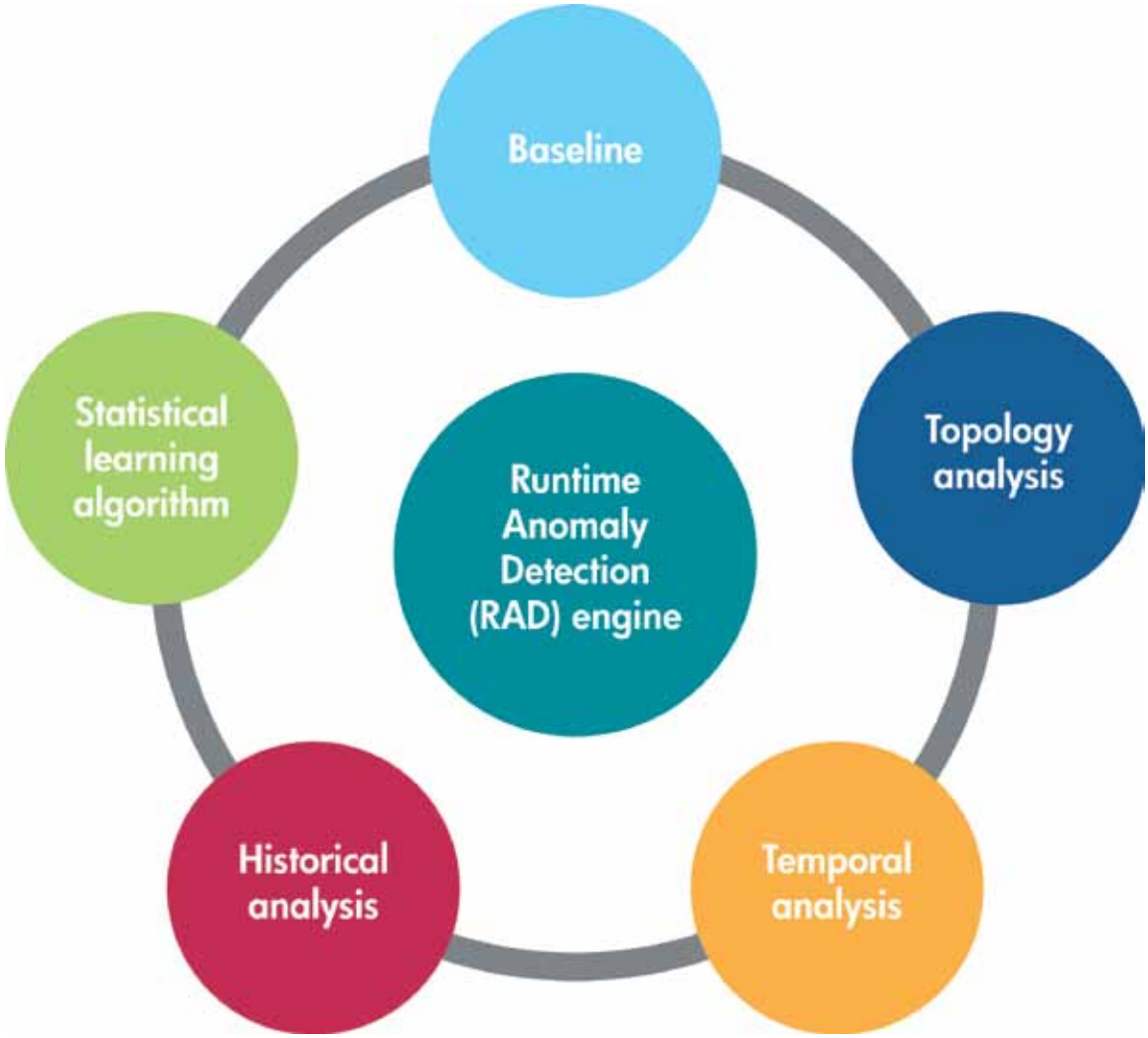
Un approccio unico: il modello di servizio HP Run-time applicato ad HP SHA

I sistemi di monitoraggio rilevano misurazioni ed eventi a tutti i livelli dello stack IT: hardware, SO di rete, middleware, applicazioni, servizi aziendali e processi. Il modello che collega tra loro tutti i diversi componenti è dato dai database di gestione configurazioni (CMDB) . Ma data il continuo mutamento insito nei sistemi IT, i database CMDB devono essere continuamente aggiornati, come avviene nel modello di servizio HP Run-time (RtSM). La combinazione tra i monitor e i CMDB in tempo reale fornisce tutti i dati necessari per rispondere alle sfide citate in apertura. Resta il fatto che tutti i dati poi devono essere trasformati per essere tradotti in informazioni usufruibili concretamente. HP SHA impiega algoritmi avanzati che riuniscono varie discipline - topologia, analisi dei dati, 'graph teory' e statistica - Run-time Anomaly Detection (RAD) Engine (Motore RAD).

La soluzione individuata da HP per i modelli di servizio obsoleti è HP RtSM. RtSM si sincronizza con HP UCMDB per sfruttare i modelli di servizio contenuti in questo database CMDB universale "esterno". L'RtSM a sua volta fa leva sui data collector della soluzione HP Business Service Management, che monitorano continuamente prestazioni, disponibilità, errori e topologia, per ottenere in tempo reale le informazioni che forniscono il quadro più aggiornato della topologia e delle relazioni. L'RtSM è uno dei pilastri di SHA.

Per maggiori informazioni su come l'RtSM utilizza UCMDB consultare la "RtSM best practices guide"

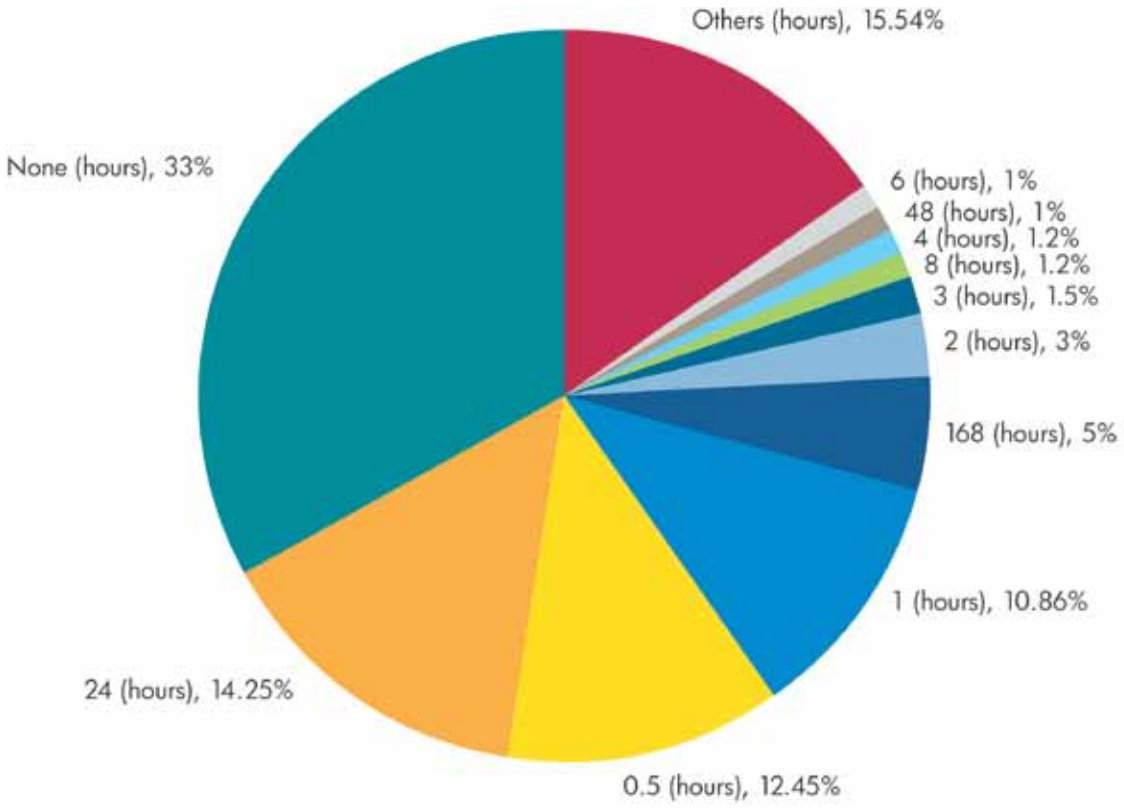
Figura 1. Modello di soluzione



La figura 1 indica i componenti di SHA necessari per una soluzione accurata di decodifica dei problemi prestazionali dell'IT. Di seguito si elencano i componenti e i rispettivi requisiti.

Baselining, o determinazione dei valori base, rappresenta la prima componente, che riunisce le varie metriche raccolte dai sistemi di monitoraggio e ne "apprende" il comportamento normale. Ogni scostamento dal comportamento normale della metrica fa scattare le attività di rilevamento, previsione e decodifica dei problemi prestazionali. L'"apprendimento" del comportamento normale delle metriche non è un compito facile. Considerate le variazioni periodiche e tendenziali e i cambiamenti intrinseci nella continua evoluzione dei sistemi IT, l'algoritmo di apprendimento che valuta qual è il comportamento normale (baseline) deve essere adattativo e consapevole di questi fattori. La figura 2 mostra la distribuzione periodica relativa a oltre 17.000 metriche prestazionali raccolte da un sistema IT reale. Le metriche abbinano monitoraggi a livello di sistema, applicazione e utente. Come si nota oltre due terzi delle metriche mostra un qualche tipo di comportamento periodico, il quale peraltro è riferito a una gamma di periodicità molto più ampia rispetto al semplice periodo gionaliero o settimanale solitamente considerato. Per essere accurato l'algoritmo per la determinazione della baseline deve in primo luogo valutare il periodo; ad esempio, se una metrica mostra un comportamento priodico di cinque ore, e l'algoritmo di baselining ignora tale periodo o ne utilizza uno predeterminato e non corretto (ad esempio 24 ore), la baseline sarà carente. E quindi sarà o troppo sensibile, e produrrà molti falsi scostamenti dalla norma in realtà normali, o troppo indiscriminato e non rileverà scostamenti dalla norma di importanza sostanziale.

Figura 2. Distribuzione del comportamento priodico di oltre 17.000 metriche raccolte in un ambiente IT



Per determinare una buona baseline è altresì importante valutare le tendenze e mantenere un grado di adattabilità ai cambiamenti.

Per quanto importante, comprendere il comportamento normale delle singole metriche non è sufficiente a rivelare e prevedere i problemi reali. Per definizione una piccola frazione di scostamenti dalla baseline non indica la presenza di potenziali di problemi effettivi; in ambienti IT complessi, con milioni di metriche, questa piccola frazione di scostamenti "innocui", se singolarmente trattata come problema, può scatenare molti falsi allarmi. Inoltre va considerato che solitamente i problemi in un ambiente non si manifestano attraverso una sola metrica.

Analisi temporale: rappresenta uno degli approcci più diffusi per combinare le metriche in una singola anomalia. I metodi improntati all'analisi temporale includono correlazioni tra metriche, dove le metriche vengono raggruppate in base alla similarità delle misure rispettivamente rilevate sulla serie temporale, o all'analisi /previsione temporale multivariata che combina diverse metriche attraverso un modello matematico multivariato, solitamente lineare, come nei modelli di regressione multivariata, neurali e bayesiani.

Tutti questi metodi sono estremamente efficaci ma hanno anche i loro limiti. In primo luogo hanno una limitata scalabilità con il numero di metriche. Poi, trattandosi di metodi statistici, di fronte a un numero molto elevato di metriche prive di relazioni reciproche reali possono individuare correlazioni fuorvianti; questa probabilità di individuare correlazioni errate aumenta all'aumentare del numero di metriche.

Analisi topologica: Ciò che consente di superare i limiti dei metodi temporali è dato dal contesto di dominio.
In particolare negli ambienti IT, l'insieme delle metriche analizzate dovrebbe limitarsi a un set logico di misurazioni correlate. Se il livello di utilizzo delle CPU di due server, privi di qualunque relazione tra loro, aumenta nello stesso momento, i dati non dovrebbero essere considerati correlati, anche se statisticamente potrebbe sembrare che lo siano. Il contesto è fornito dalla topologia dei sistemi IT attraverso i database CMDB. Un CMDB è essenzialmente un grafico che modella le relazioni tra tutti i componenti che costituiscono i sistemi IT, a livello fisico, middleware, software, applicazioni, servizi e processi business. L'analisi della topologia, sotto forma di algoritmi grafici avanzati, consente pertanto di estrarre le informazioni contestuali all'interno del CMDB, e contribuisce alla rilevazione dei problemi reali e delle correlazioni tra le metriche, con filtraggio del rumore.

Per individuare un problema reale, quindi, bisogna rilevare i modelli di scostamento dalla normalità di molteplici metriche nel tempo, filtrati in base alla topologia. Ciò consente di ottenere metodi di apprendimento statistici che considerano i dati temporali e topologici.

Analisi storica: oltre al rilevamento e alla previsione di un problema, la topologia consente di valutarne la portata e di distinguere di fondo dai sintomi; due aspetti essenziali per una risoluzione rapida dei problemi. Dopo che il problema è stato rilevato e analizzato, il suo DNA viene infine decodificato, e il tutto può essere archiviato in un'apposita base di conoscenze. Per utilizzare questa base di conoscenze occorrono algoritmi in grado di eseguire un'analisi storica. Tra questi vi sono quelli che consentono di confrontare, comparare e raggruppare i modelli di DNA dei diversi problemi e le tecniche di classificazione. Una volta creata la base di conoscenze e sviluppati gli algoritmi, i problemi passati possono essere utilizzati in modo rapido e automatico per contribuire a determinare le root-cause dei nuovi problemi e a risolverli.

Motore RAD: il motore RAD è definito da questo set completo di algoritmi. Gli algoritmi nel motore RAD sono coperti da 10 diverse richieste di brevetto. L'output del motore RAD rappresenta un indicatore prestazionale chiave (KPI) nella dashboard di HP BSM, e attiva l'invio di un evento nel sottosistema eventi di BSM, HP Operations Manager i (OMi). L'evento originato da SHA contiene una quantità di informazioni contestuali raccolte dal motore RAD, tra cui i principali sospetti, informazioni sull'ubicazione, informazioni sull'impatto aziendale, un elenco degli elementi di configurazione (CI) implicati nell'anomalia e altre informazioni utili sull'anomalia. Queste informazioni aiutano il cliente a isolare e risolvere l'evento rapidamente prima che possa impattare le attività.

L'analisi previsionale in tempo reale di HP SHA

All'interno di SHA gli algoritmi di apprendimento statistici sono abbinati ad algoritmi grafici che consentono di analizzare l'intero spettro di dati raccolti dai sistemi di BSM:

- Dati di monitoraggio (utenti di sintesi e reali)
- Eventi
- Modifiche
- Topologia rilevata dall'RtSM

Questi algoritmi rilevano con precisione le anomalie, ne decodificano la struttura genetica e l'impatto aziendale, e li confrontano con le anomalie rilevate in precedenza riunite nella base di conoscenze sul DNA delle anomalie (Anomaly DNA Knowledgebase).

Il sistema SHA può essere descritto attraverso i seguenti passaggi:

- **Apprendimento del comportamento delle metriche**

  Il primo passo indispensabile è l'apprendimento del comportamento normale, o "baselining", delle metriche raccolte a tutti i livelli del servizio (sistema, middleware, applicazione e altri). Questo passaggio elimina l'esigenza di stabilire delle soglie statiche per le metriche e consente un rilevamento precoce degli scostamenti dalla normalità. I principali punti di forza dei nostri algoritmi sono:

  – **Apprendimento** automatico del comportamento periodico delle metriche e delle relative tendenze
  – **Adattabilità** alle modifiche del comportamento nel tempo: un elemento imprescindibile negli ambienti virtualizzati
  – **Zero configurazioni**: per stabilire o gestire le soglie non occorrono attività di amministrazione

- **Tecnologia Anomaly DNA: rilevamento**

  Quando in un servizio IT si sviluppa un problema olistico, numerose metriche e componenti collegate con tale servizio iniziano a registrare degli scostamenti rispetto alla norma. Tuttavia vari componenti subiscono continuamente scostamenti temporanei dalla norma che non rappresentano problemi significativi. La vera sfida per qualunque sistema di rilevamento delle anomalie sta nel selezionare i problemi significativi e nell'individuare il DNA dei problemi reali. Il nostro algoritmo di rilevamento del DNA delle anomalie ci riesce grazie a un esclusivo algoritmo statistico che abbina tre tipi di informazioni per garantire un rilevamento accurato:

  – **Informazioni topologiche**: collegamenti logici tra i monitor e i componenti da essi monitorati
  – **Informazioni temporali**: la durata e la correlazione temporale dei parametri di monitoraggio che risultano anomali
  – **Informazioni sull'affidabilità statistica**: la probabilità che un parametro di monitoraggio risulti effettivamente anomalo, in base a quanto appreso rispetto alla baseline, nel tempo

I principali punti di forza del nostro algoritmo di rilevamento delle anomalie sono:

- **Riduzione delle congestioni**: offre un metodo automatico per raggruppare le metriche, che hanno sforato la propria baseline, che utilizza informazioni temporali e topologiche. Ciò a sua volta riduce il numero di sforamenti rispetto alla baseline che l'operatore deve effettivamente controllare, senza il bisogno di stabilire alcuna regola specifica.
- **Riduzione degli eventi**: gli algoritmi di SHA riuniscono varie metriche anomale in un solo evento, riducendo quindi il numero totale di eventi presentati all'operatore. L'avvio per questo tipo di eventi è rappresentato dalla violazione delle soglie dinamiche relative a più metriche. SHA correla queste metriche in termini di tempo e di topologia per generare un solo evento, consentendo in tal modo all'operatore di concentrarsi sul problema effettivo.
- **Riduzione dei falsi allarmi**: calcolando la significatività delle singole anomalie del sistema, attraverso un algoritmo statistico, si riducono i falsi allarmi. Le anomalie correnti vengono confrontate anche con le anomalie note che in passato sono state classificate come rumore, con eventuale soppressione dell'evento anomalo.

- **Tecnologia Anomaly DNA: decodifica**

  Il passaggio successivo nel rilevamento dell'anomalia e della sua struttura è la decodifica del DNA. La decodifica del DNA dell'anomalia è realizzata analizzandola e classificandola in base alla topologia (CI e relativa struttura topologica), alle metriche e ad altre informazioni. La decodifica, in particolare, consente di:
  - Separare i sospetti, in modo da fornire informazioni applicabili nella pratica. Identificare l'impatto aziendale utilizzando le informazioni collegate con il business: volume di utenti, SLA (service-level agreements) e aree geografiche interessate; ciò consente di stabilire la priorità dell'anomalia a seconda dell'impatto
  - Identificare le modifiche collegate che potrebbero aver influenzato il comportamento del sistema

- **Tecnologia Anomaly DNA: confronto**

  Una volta decodificato il DNA dell'anomalia il sistema esegue il confronto dell'anomalia corrente con quelle passate. Il confronto viene eseguito con un esclusivo algoritmo grafico di similarità che confronta le strutture astratte delle anomalie individuando le corrispondenze tra le anomalie rilevate nei diversi servizi che possiedono un'architettura simile. Questa modalità di confronto presenta diversi vantaggi:
  - Consente di riutilizzare le soluzioni individuate per eventi passati.
  - Esegue il confronto con le anomalie collegate con problemi noti e ancora insoluti, riducendo l'esigenza di ripetere le indagini
  - Riduce i falsi allarmi quando un'anomalia passata simile è stata classificata come rumore, ad esempio quando l'anomalia stessa è causata da normali attività di manutenzione del servizio

- **Anomaly DNA Knowledgebase**

  Via via che si forma la base di conoscenze sulle anomalie passate e la relativa risoluzione, questa utilizzando metodi di data mining avanzati analizza e genera le relazioni tra tutte le anomalie, creando in tal modo una mappa dell'intera Anomaly DNA Knowledgebase. Il nostro algoritmo di confronto del DNA delle anomalie definisce lo spazio metrico richiesto per i metodi di data mining come raggruppamento e classificazione. L'applicazione di tali metodi offre i seguenti benefici:
  - Risoluzione proattiva dei problemi, identificazione dei problemi ricorrenti tramite la classificazione del DNA delle anomalie in base al tipo di problema e di risoluzione. Riduce i tempi necessari a diagnosticare e risolvere queste tipologie di problemi in futuro
  - Utilizzo delle conoscenze raccolte a partire da vari servizi che mostrano un comportamento simile

Capacità del prodotto

Sviluppato sulla base di HP RtSM, HP SHA analizza le tendenze e i valori normali storici relativi alle applicazioni e all'infrastruttura, e li confronta con le metriche di prestazione in tempo reale. L'utilizzo di un modello di servizio in tempo reale è essenziale negli ambienti dinamici perché permette di:

- Correlare le anomalie con le modifiche della topologia e i problemi passati
- Comprendere l'impatto sul business dei singoli problemi e attribuire la corretta priorità alla risoluzione
- Identificare i sospetti responsabili del problema e utilizzare questa conoscenza per prevenire problemi simili in futuro

SHA apprende automaticamente le soglie dinamiche dell'ambiente, evitandovi di dover investire in risorse per impostare e gestire soglie statiche. SHA opera sulle metriche generate dalle seguenti sorgenti di dati BSM:

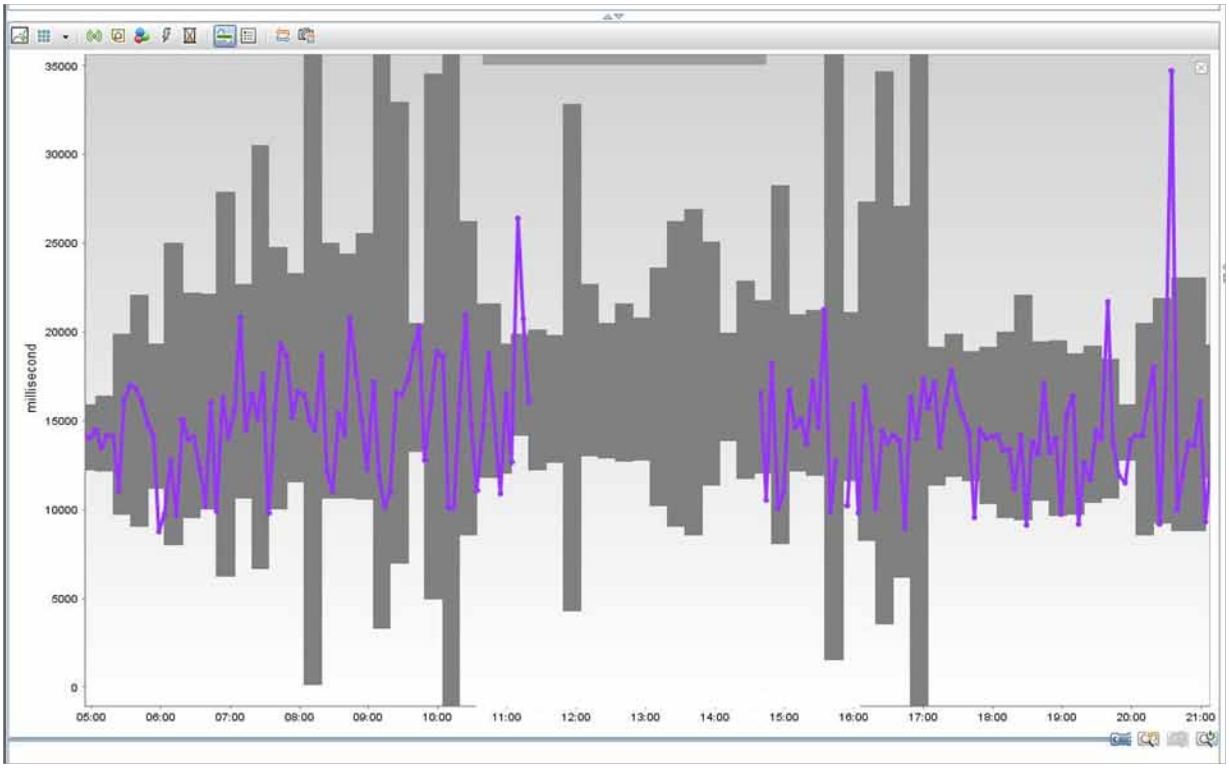
- HP Business Process Monitor
- HP Diagnostics
- HP Network Node Manager i
- HP Operations Manager, Performance Agent
- HP Real User Monitor
- HP SiteScope

SHA individua le anomalie in base al comportamento anomalo delle metriche collegate con il RtSM, stabilisce un KPI e genera un evento, completo di contesto, per facilitare la determinazione della priorità aziendale del problema. SHA inoltre utilizza la tecnologia Anomaly DNA per analizzare la struttura di un'anomalia e confrontarla con il DNA di altre anomalie conosciute. Il confronto consente di identificare gli interventi di risoluzione noti senza effettuare ulteriori indagini, mentre gli eventi contrassegnati come rumore vengono soppressi. Se viene rilevata un'anomalia in relazione a un servizio specifico, è possibile controllare il relativo SLA per determinarne il potenziale impatto. Infine SHA integra anche le funzionalità di risoluzione di HP Closed Loop Incident Process (CLIP) ed è direttamente integrato con HP Operations Orchestration. Per risolvere rapidamente i problemi, ad esempio, è possibile abbinare analisi e automazione. Quando SHA invia un evento in OMi (Operation Manager i), l'operatore attraverso il processo CLIP può intervenire prima che il servizio abbia a risentirne. Questa procedura di risoluzione rapida riduce la complessità di gestione degli ambienti virtualizzati e in cloud.

Avvio rapido con zero configurazioni e zero mantenimento

Dopo aver installato il prodotto e selezionato le applicazioni che si vogliono monitorare, SHA inizia a raccogliere i dati e ad apprendere il comportamento del sistema. Raccogliendo i dati dall'applicazione, dall'infrastruttura, dal database, dalla rete e dal middleware, oltre alle informazioni topologiche fornite dall'RtSM, SHA stabilisce la baseline. La baseline rappresenta il comportamento normale di una data metrica nel tempo, anche in considerazione delle caratteristiche di periodicità. Il comportamento normale di una metrica, in tal senso, può ad esempio comprendere il comportamento di un lunedì mattina molto intenso e di un venerdì pomeriggio piuttosto calmo.

Figura 3. Esempio di una baseline dinamica (fascia grigia) con i dati metrici effettivi (viola).

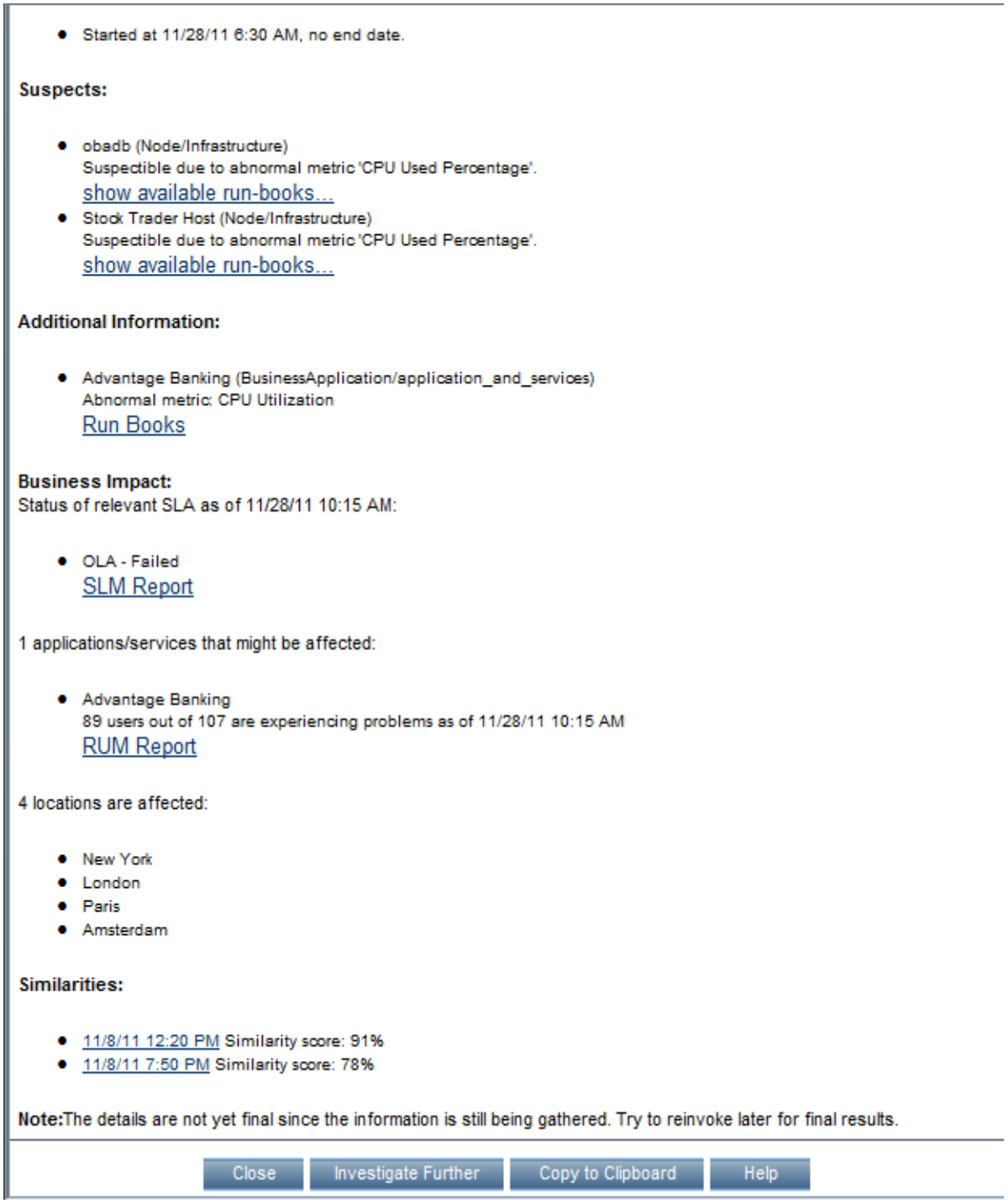


Dopo aver stabilito le baseline dinamiche per tutte le metriche dell'applicazione, il motore RAD di SHA inizia a monitorare le anomalie nel comportamento dell'applicazione. L'avvio per il motore RAD è rappresentato da una violazione della baseline tale da indicare che la metrica interessata sta mostrando un comportamento anomalo. Per definire un'anomalia il motore RAD fa riferimento alle informazioni sulle metriche anomale ricavate da tutte le metriche controllate e le abbina alle informazioni topologiche ricavate da RtSM, per determinare se si tratta di più violazioni, da parte di più metriche, riferite allo stesso servizio. Quando viene rilevata un'anomalia il sistema genera un evento e lo invia al sottosistema eventi. Inoltre, quando viene rilevata un'anomalia, SHA acquisisce automaticamente la topologia attuale dell'elemento di configurazione coinvolto nell'evento. Il vantaggio è che in questo modo è possibile comprendere lo stato della topologia al momento dell'anomalia. Questa informazione è particolarmente utile per l'analisi delle anomalie che si verificano durante la notte o quando non è disponibile personale IT in grado di risolvere il problema. SHA inoltre rileva e presenta i dati relativi alle modifiche rilevate per gli elementi di configurazione coinvolti, affinché possano essere utilizzati durante l'analisi della cause di fondo. Questa correlazione sveltisce la gestione dei problemi e riduce il tempo medio di risoluzione (MTTR).

Quando scopre un'anomalia nel comportamento dell'applicazione, SHA cambia lo stato del Predictive Health KPI e genera un evento che viene inviato al browser eventi di BSM. A partire da questo momento l'operatore può iniziare ad approfondire il livello di dettaglio, isolare il problema e comprendere il relativo impatto sulle attività aziendali.

SHA offre una pagina che sintetizza gli aspetti fondamentali del problema, e il suo impatto sull'attività, e funzionalità di isolamento avanzate che consentono di approfondire il livello di dettaglio e di indagare ulteriormente il problema.

Figura 4. Pagina di sintesi delle anomalie

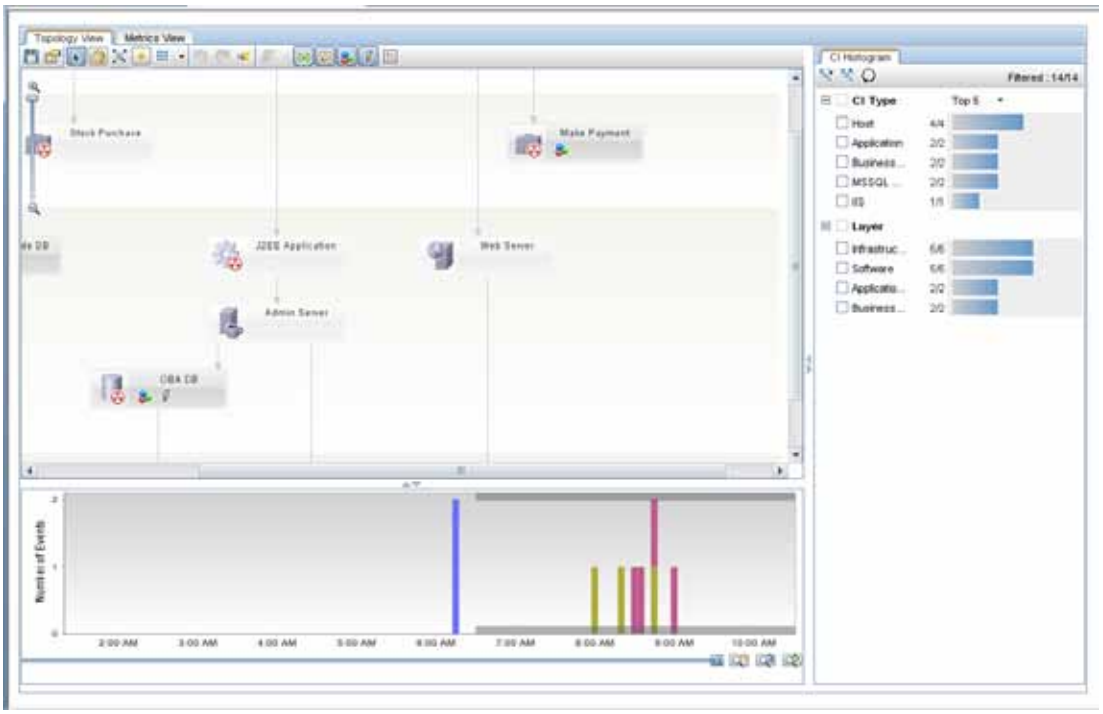


Nella parte alta della figura 4 è visibile la "lista dei sospetti". I sospetti sono gli elementi di configurazione (applicazioni, transazioni, elementi dell'infrastruttura) che secondo SHA potrebbero aver causato l'anomalia. I sospetti possono essere gli elementi di configurazione (Configuration Items) le cui metriche hanno violato la baseline, i modelli di anomalia precedentemente individuati come tali e gli elementi di configurazione che non hanno superato le verifiche effettuate con gli strumenti utilizzati dal cliente.

La pagina di sintesi inoltre indica l'impatto aziendale dell'anomalia attraverso la specificazione degli SLA violati in conseguenza dell'anomalia, dei servizi e delle applicazioni coinvolti e di un elenco delle località interessate dall'impatto. SHA inoltre propone l'esecuzione dei report del caso al fine di approfondire il livello di dettaglio per migliorare la comprensione del problema. La sezione delle anomalie simili, generata attraverso la tecnologia Anomaly DNA, rafforza le informazioni sull'occorrenza del problema mostrando un elenco di modelli analoghi e altre indicazioni su come sono stati gestiti nel passato.

SHA presenta un'interfaccia utente che offre uno strumento di indagine e isolamento dei problemi con cui è possibile approfondire il livello di dettaglio sull'anomalia e circoscrivere la possibile root-cause del problema: la Subject Matter Expert User Interface (SME UI). Questo strumento di indagine permette di "viaggiare nel tempo" all'interno dell'anomalia per avere una visione dettagliata della serie di eventi che hanno portato al problema, rispecchiata dalla topologia dell'applicazione. La figura qui sotto mostra un esempio di anomalia e della relativa serie di eventi nel tempo.

Figura 5. SME UI con la schermata della topologia di un'anomalia



La parte inferiore dello schermo mostra gli eventi verificatisi nel sistema e acquisiti da SHA nel tempo, prima e durante l'anomalia.

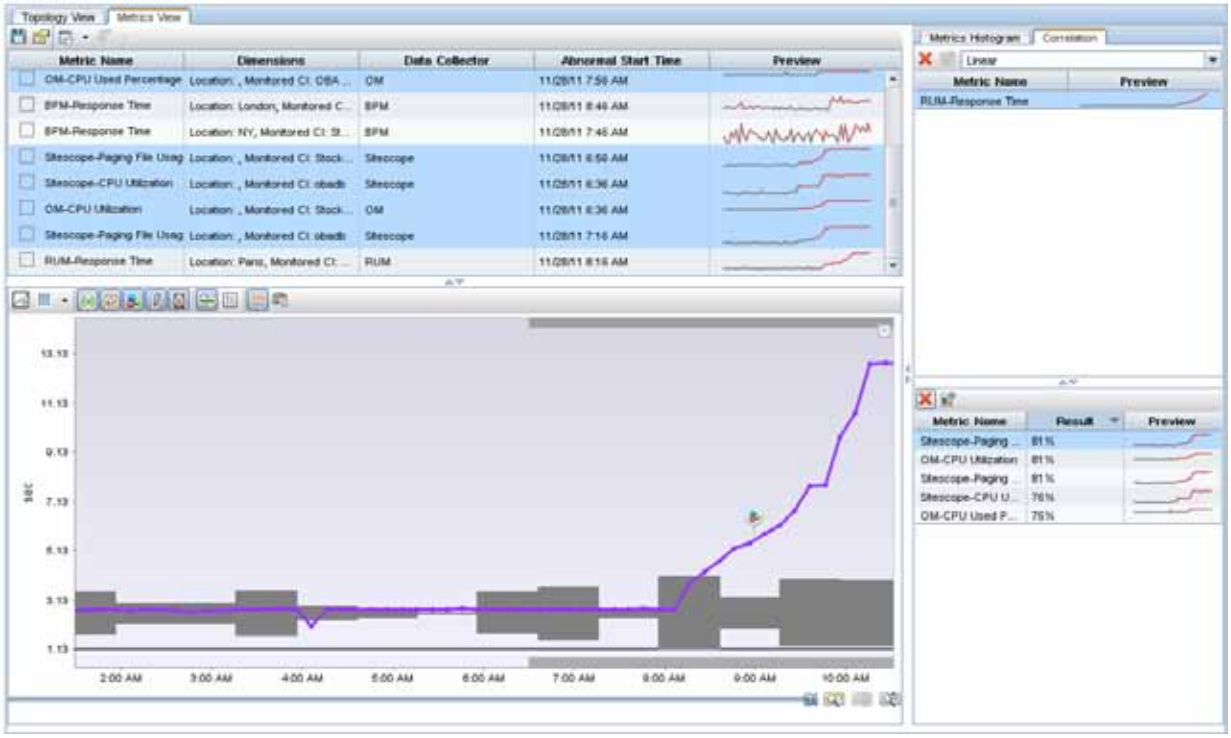
- Alle 06:15 SHA ha registrato una modifica rilevata nel sistema.
- Alle 06:30 SHA ha attivato un'anomalia. Ciò significa che ha rilevato delle metriche anomale in violazione delle rispettive baseline, **prima che** SiteScope e OM, impegnati a monitorare il sistema in parallelo, rilevassero il fatto. A questo punto SHA **ha già attivato un evento, inviandolo al personale operativo**.
- Alle 08:00 – 08:20 SiteScope e OM hanno attivato eventi basati sull'elevato utilizzo della CPU. Il motivo per cui SiteScope e OM hanno rilevato il problema **più tardi di SHA** è che le rispettive soglie sono state fissate a un punto più alto rispetto alla baseline dinamica di SHA, al fine di ridurre il rumore e allarmi positivi falsi.
- Alle 8:30 il primo utente reale ha constatato il problema prestazionale e ha aperto un incidente.

Come si vede SHA ha scoperto il problema e ha lanciato l'avviso **con due ore di anticipo** e prima che un qualunque utente se ne lamentasse, notificando precocemente al personale operativo la necessità di gestirlo e risolverlo.

SHA offre un poderoso strumento per correlare e individuare le metriche che potrebbero essere alla radice dei problemi nel sistema.

La figura qui sotto illustra la schermata delle metriche di SHA fornita nell'ambito della SME UI.

Figure 6. Schermata delle metriche di SME UI



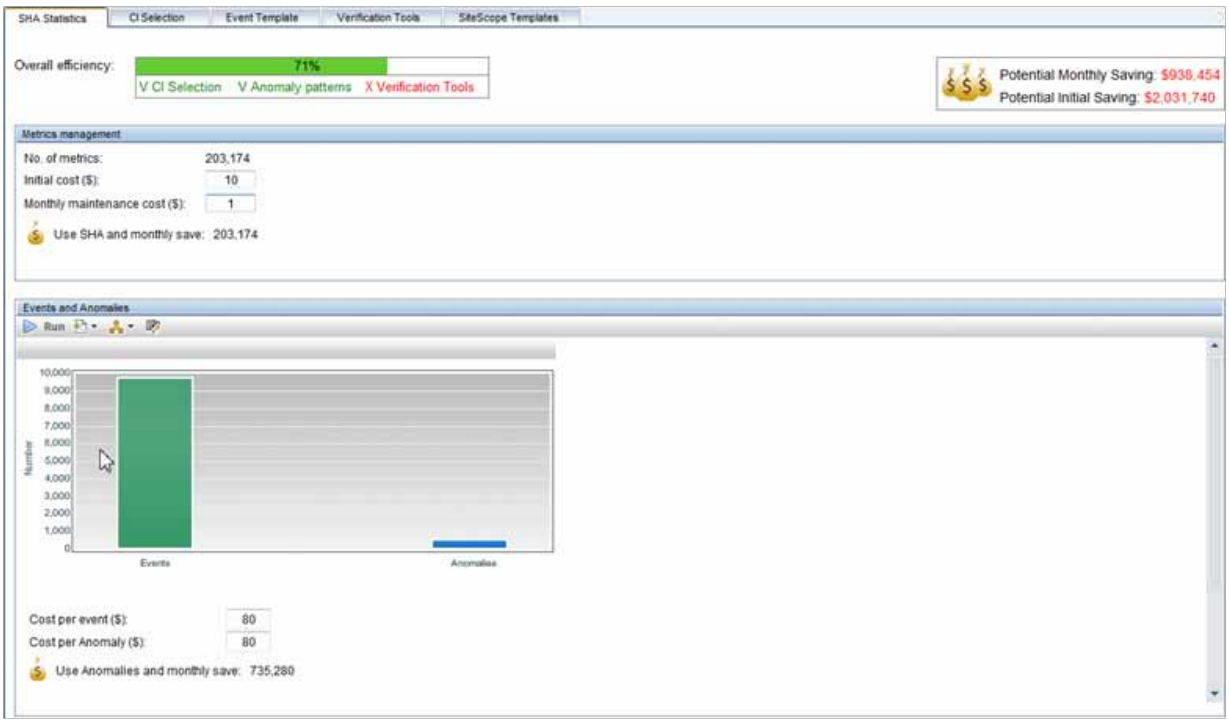
La "metric view" offre un'anteprima delle metriche relative all'applicazione rilevate durante l'intervallo di tempo dell'anomalia nel “quadro” delle rispettive baseline. Essa inoltre consente di individuare le metriche alla base del problema correlandole alle altre collegate con lo stesso servizio mediante algoritmi statistici sofisticati.

In questo esempio l'utente ha deciso di correlare la metrica Real User Monitor (RUM) con tutte le altre. La scelta di questa metrica si deve al fatto che è quella che meglio rappresenta il tempo di risposta reale che gli utenti effettivi sperimentano utilizzando l'applicazione. Le altre si riferiscono ai componenti dell'infrastruttura e del middleware; la schermata delle metriche offre un semplice meccanismo point-and-click per presentare una correlazione tra le metriche stesse e il tempo di risposta scadente. La metrica che ha ottenuto il valore di correlazione più alto (81%) è “Sitescope_paging File Usage”, che indica che la causa di fondo molto probabilmente è un'allocazione di memoria insufficiente.

Ritorno sull'investimento

SHA calcola il ritorno sull'investimento (ROI) utilizzando le informazioni raccolte dall'ambiente di distribuzione. La sezione gestione delle metriche esamina il ROI collegato con la riduzione delle attività di impostazione e gestione delle soglie reso possibile dalla capacità di apprendimento automatico delle soglie dinamiche di SHA. La sezione eventi e anomalie considera il ROI collegato con la riduzione degli eventi comparando l'attuale flusso di eventi di OMi con gli eventi basati sulle anomalie da SHA. Queste informazioni sono riassunte in termini di efficienza complessiva.

Figura 7. Schermata del ROI di Service Health Analyser



Conclusione

SHA è la soluzione HP di nuova generazione per l'analisi previsionale in tempo reale capace di individuare i problemi IT prima che si verifichino, analizzando i comportamenti anomali dei servizi e segnalando ai responsabili IT i cali di prestazioni reali prima che possano influire sui processi di business. Grazie a una stretta integrazione con le soluzioni HP BSM per la risoluzione degli eventi, SHA riduce l'MTTR.

Inoltre è facile da usare, minimizza le attività di impostazione e configurazione e si impara con la massima facilità. SHA elimina l'esigenza di gestire le soglie di monitoraggio, perché apprende continuamente il comportamento delle applicazioni e regola le soglie delle metriche di conseguenza. Il sistema riduce il tempo medio di risoluzione dei problemi nelle applicazioni e segnala solo i problemi reali indicando le possibili root-cause. Sviluppato sulla base del modello di servizio dinamico HP RtSM, SHA aiuta gli operatori IT a individuare i potenziali problemi a livello di topologia e servizi e a risolverli prima che si manifestino con disservizi per gli utenti finali.

HP Service Health Analyser (HP SHA) rappresenta la nuova era dell'analisi in campo IT. Per ulteriori informazioni visitare il sito www.hp.com/go/sha.

4AA3-8672ITE, data di creazione: dicembre 2011