HP Service Health Analyzer : Decoding the DNA of IT Performance Problems (Décodage de l'ADN des problèmes de performance informatique)

Livre blanc technique

Table des matières

Introduction

Ce n'est pas seulement nice-to-have d'avoir la garantie d'une visibilité complète sur la santé de vos services métiers, de pouvoir s'adapter, voire de survivre dans l'environnement informatique virtualisé et de cloud actuel. C'est aussi obligatoire. La gestion d'une infrastructure et d'applications dynamiques nécessitera davantage qu'une simple réaction aux problèmes des services métiers lors de leur apparition, ou que la mise à jour manuelle des seuils statiques dont la définition précise est difficile et la maintenance problématique.

Dans le monde actuel, la notification avancée des problèmes vous est nécessaire afin de pouvoir les résoudre avant que votre business ne soit impacté. Vous avez besoin d'une meilleure visibilité sur la manière dont vos applications et services métiers sont corrélés avec votre infrastructure dynamique de façon à pouvoir surveiller les anomalies sur l'ensemble de la couche informatique, notamment le réseau, les serveurs, les middlewares, les applications et les processus métiers. Vous avez besoin d'un moyen plus simple pour déterminer les seuils acceptables comme base d'identification des événements qui peuvent avoir un impact métier. Vous avez besoin de l'automatisation pour exploiter des connaissances issues d'événements antérieurs afin d'aborder plus efficacement les nouveaux événements, supprimer les événements extérieurs, ce qui permet à l'informatique de se concentrer uniquement sur les événements qui ont un impact métier.

Bien que les services informatiques possèdent des méthodes de collecte de quantités massives de données, ce qui leur a manqué, c'est le kit d'outils analytiques et l'intelligence automatisée permettant de corréler ces mesures disparates du point de vue d'une application et d'une topologie pour aider ces services informatiques à anticiper ou à prévoir les problèmes potentiels avant qu'ils se produisent. Les responsables informatiques étudient le domaine de l'analyse prédictive, l'une des grandes tendances en matière de business intelligence en 2011, afin d'améliorer la disponibilité et les performances du service, augmentant ainsi le chiffre d'affaires de l'entreprise et réduisant les coûts de maintenance et de support.

HP Service Health Analyzer (SHA) est un outil d'analyse prédictif basé sur un modèle de service dynamique en temps réel, qui vous permet de comprendre la relation entre les anomalies de métrique avec l'application et son infrastructure sous-jacente.

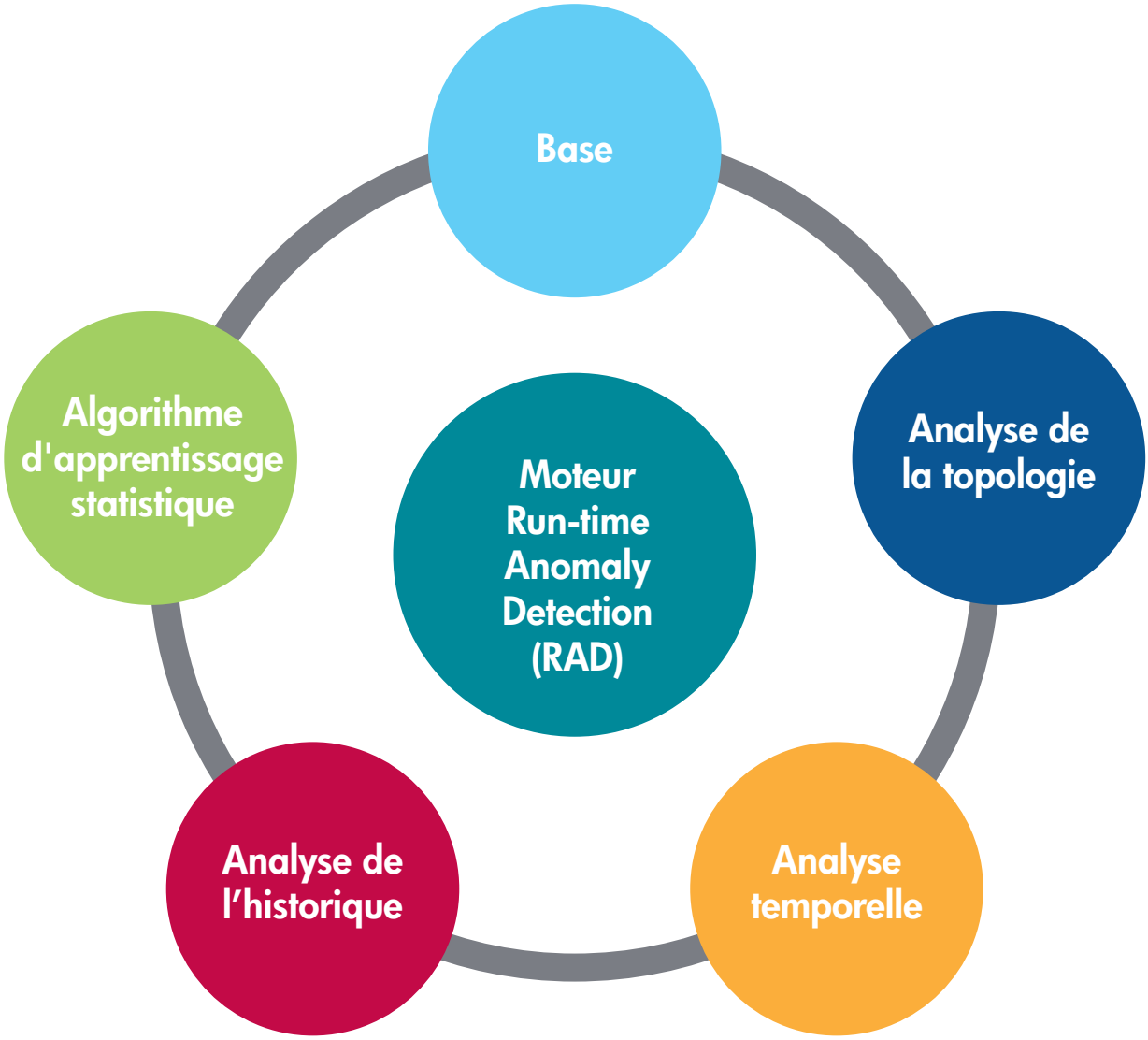
Une approche unique — HP SHA guidé par le modèle HP Run-time Service Model

Les systèmes de surveillance offrent des mesures et des événements à partir de toutes les couches du système d'informations : matériel, système d'exploitation du serveur, middlewares, applications, services métiers et processus métiers. Les bases de données de gestion des configurations (CMDB) fournissent le modèle qui relie tous les différents composants. Cependant, au vu de la nature versatile des systèmes informatiques, les CMDB doivent être mises à jour en permanence, comme dans le cas du modèle HP Run-time Service Model (RtSM). La combinaison des moniteurs et de la base de données CMDB en temps réel offre toutes les données nécessaires permettant de relever les défis ci-dessus. Toutefois, l'ensemble des données doit être transformé pour fournir des informations pertinentes. La solution HP SHA utilise des algorithmes avancés qui associent plusieurs disciplines, la topologie, l'analyse des données, la théorie des graphes et les statistiques dans le moteur RAD (Run-time Anomaly Detection).

La solution HP au modèle de service obsolète est notre RtSM. Le modèle RtSM est synchronisé avec la base de données HP UCMDB afin d'optimiser la modélisation du service dans la base de données universelle de gestion des configurations (UCMDB) "externe". Le modèle RtSM optimise ensuite les collecteurs de données du portefeuille HP Business Service Management (BSM), qui surveillent les performances, la disponibilité, les anomalies et la topologie pour partager la topologie "en temps réel" afin que le modèle RtSM ait la compréhension la plus à jour de la topologie et de ses relations. Le moteur RtSM est le cœur de la solution SHA.

Pour plus d'informations sur le fonctionnement de RtSM avec l'UCMDB, consultez le "guide des meilleures pratiques du modèle RtSM".

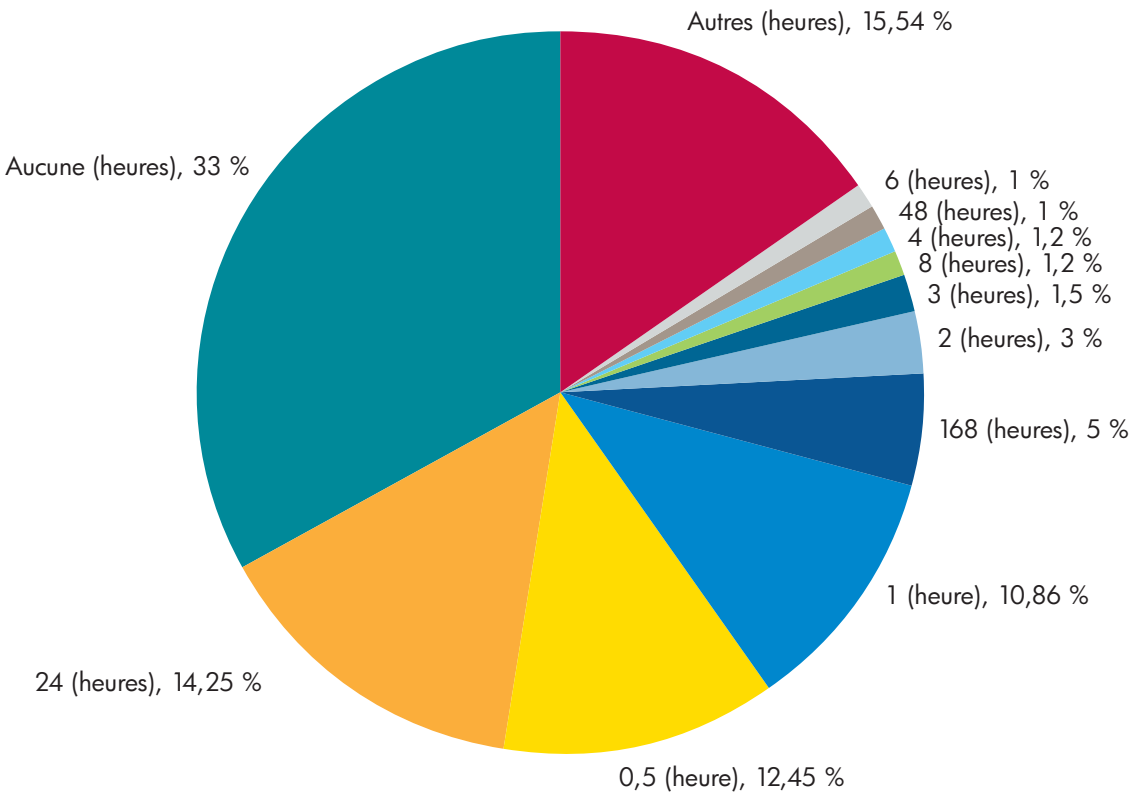
Figure 1. Modèle de la solution



La figure 1 montre les composants du SHA requis pour une solution précise de décodage des problèmes de performance informatique. Nous allons maintenant décrire les composants et leurs exigences.

La **base de référence** est le premier composant, qui prend chaque mesure collectée par les systèmes de surveillance pour en apprendre davantage sur son comportement normal. Les écarts par rapport au comportement normal représentent la première étape de détection, de prévision et de décodage des problèmes de performance. Cependant, le fait de connaître avec précision le comportement normal des mesures est une tâche difficile. Des facteurs tels que le comportement périodique, les tendances et les changements dus à un système informatique en évolution constante nécessitent que l'algorithme d'apprentissage estimant la base de référence s'adapte et soit conscient de ces facteurs. La figure 2 montre la répartition de la période pour plus de 17 000 mesures de performance collectées à partir d'un système informatique réel. C'est une combinaison entre le système, l'application et les moniteurs au niveau de l'utilisateur. Plus des deux tiers des mesures présentent un comportement périodique, ce qui représente une plage de différentes périodes et pas seulement la périodicité quotidienne ou hebdomadaire généralement supposée. Un algorithme de référence doit d'abord estimer la période de référence pour être précis. Par exemple, si une mesure présente un comportement relatif à une période de cinq heures et si un algorithme de référence ignore la période de référence ou utilise une période prédéfinie qui est incorrecte (comme 24 heures), une base de référence médiocre sera produite. La base de référence sera trop sensible, générant de nombreux écarts incorrects par rapport au comportement normal (qui sont en fait normaux). Elle pourra aussi être trop systématique et ne détectera pas les écarts par rapport au comportement normal, le cas échéant.

Figure 2. Répartition du comportement périodique pour plus de 17 000 mesures collectées à partir d'un environnement informatique



De la même façon, l'évaluation de la tendance et l'adaptation aux changements sont importantes pour estimer une base de référence appropriée.

Bien que la compréhension du comportement normal des mesures individuelles soit importante, elle n'est pas suffisante pour détecter et prévoir les problèmes réels. Par définition, certains écarts par rapport à la base de référence ne sont pas liés à un problème (une petite fraction). Et dans un vaste environnement informatique avec des millions de mesures, même cette petite fraction peut entraîner l'apparition d'un nombre trop important de fausses alertes, s'ils sont traités individuellement comme un problème. De plus, les problèmes ne se manifestent généralement pas sur une seule mesure de l'environnement.

Analyse temporelle : c'est l'une des approches générales permettant de combiner les mesures dans une seule anomalie. Les méthodes d'analyse temporelle comprennent les corrélations de mesure à mesure, dans lesquelles les mesures sont regroupées en fonction de la similitude de leurs mesures de série temporelle, ou l'analyse/la prévision temporelle multiple qui combine plusieurs mesures via un modèle mathématique multiple et généralement linéaire, comme la régression multiple, la régression neuronale et les modèles bayésiens.

Ces méthodes sont puissantes, mais elles ont également leurs limites. Tout d'abord, elles évoluent mal avec le nombre de mesures. Ensuite, au vu de leur nature statistique, ces méthodes peuvent trouver des corrélations trompeuses si un grand nombre de mesures leur est fourni, sans aucune véritable relation entre elles. La probabilité de trouver ces corrélations incorrectes augmente avec le nombre de mesures.

Analyse de la topologie : ce qui aide les méthodes temporelles à surmonter leurs limites, c'est un contexte lié au domaine. Dans les environnements informatiques en particulier, le jeu des mesures qui est analysé doit être limité à un jeu logique de mesures liées. Si les processeurs de deux serveurs sans aucun rapport sont en période de pointe en même temps, ils ne doivent pas être considérés comme corrélés même si, statistiquement, ils semblent l'être. Ce contexte est fourni dans la topologie des systèmes informatiques via les bases de données CMDB. Une base de données CMDB est essentiellement un graphique qui modélise les relations entre tous les composants des systèmes informatiques : les couches physiques, les middlewares, les logiciels, les applications, les services métiers et les processus métiers. Par conséquent, l'analyse de la topologie, sous la forme d'algorithmes de graphique avancés, est requise pour extraire les informations contextuelles dans la base de données CMDB et pour aider à détecter les problèmes réels et les corrélations entre les mesures lors du filtrage du bruit.

C'est pour cette raison que la détection d'un problème réel nécessite la détection des modèles d'écarts par rapport à la normalité de plusieurs mesures qui s'étendent dans le temps et qui sont filtrées par la topologie. Cela donne les méthodes d'apprentissage statistique qui analysent les données temporelles et topologiques.

Analyse de l'historique : au-delà de la détection et de la prévision d'un problème, la topologie permet d'évaluer l'ampleur du problème et de séparer la cause première des symptômes. Les deux sont importantes pour résoudre rapidement les problèmes. Avec la détection et l'analyse d'un problème, son modèle d'ADN est finalement décodé et il peut être stocké dans une base de connaissances. Pour tirer parti de la base de connaissances, les algorithmes qui effectuent l'analyse d'historique sont requis. Ils incluent les algorithmes permettant de faire correspondre et de comparer les différents modèles d'ADN des problèmes, leur regroupement, ainsi que des techniques de classification. Avec la base de connaissances et les algorithmes en place, les problèmes peuvent être rapidement et automatiquement optimisés pour trouver la cause première et les résolutions aux nouveaux problèmes.

Moteur RAD : il est défini par ce jeu complet d'algorithmes. Les algorithmes dans le moteur RAD sont l'objet de 10 applications de brevet distinctes. Les données de sortie du moteur RAD sont un indicateur de performance clé (KPI) critique dans le tableau de bord HP BSM qui envoie un événement au sous-système d'événements BSM, HP Operations Manager i (OMi). L'événement issu de SHA contient un grand nombre d'informations contextuelles recueillies par le moteur RAD, notamment les principaux éléments suspects, les informations sur les sites, les informations sur l'impact métier, une liste des éléments de configuration (CI) impliqués dans l'anomalie, ainsi que toutes les informations sur les anomalies similaires. Ces informations permettront aux clients d'isoler et de résoudre rapidement l'événement avant que le business soit impacté.

HP SHA — Analyse prédictive d'exécution

Dans la solution SHA, nous avons développé des algorithmes d'apprentissage statistique, associés à des algorithmes de graphiques, pour analyser l'ensemble des données collectées par les produits BSM :

- Surveillance des données (synthétique et Real User)
- Événements
- Changements
- Topologie du modèle RtSM

Ces algorithmes détectent avec précision les anomalies, décodent leur structure d'ADN, leur impact métier et les font correspondre aux anomalies détectées auparavant et recueillies dans notre base de connaissances d'Anomaly DNA.

La solution SHA peut être décrite dans les étapes suivantes :

- **Apprentissage du comportement des mesures**

  L'apprentissage du comportement normal, également considéré comme base de référence, des mesures recueillies depuis tous les niveaux du service (système, middlewares, applications, etc.) est une première étape indispensable. Elle élimine le besoin de définir des seuils statiques et permet de détecter à l'avance les écarts par rapport à la normalité. Les principaux atouts de nos algorithmes sont les suivants :
  - Apprentissage **automatique** du comportement périodique des mesures et sa tendance
  - **Adaptation** aux changements comportementaux au fil du temps (un must dans les environnements virtualisés)
  - **Aucune configuration** : aucun effort d'administration n'est requis pour définir ou maintenir les seuils

- **Anomaly DNA Technology — Détection**

  Lorsqu'un problème holistique évolue dans un service informatique, de nombreux composants et mesures liés à ce service commencent à présenter des écarts par rapport au comportement normal. Cependant, il est possible de trouver des écarts momentanés constants par rapport à la normalité, par différents composants qui ne constituent pas un problème significatif. La sélection des problèmes significatifs et la recherche de l'ADN des problèmes réels représentent un défi pour tous les systèmes de détection des anomalies. Notre algorithme de détection de l'ADN des anomalies y parvient à l'aide d'un algorithme statistique unique, qui combine trois types d'informations nécessaires à la réalisation d'une détection précise :
  - **Topologique** : liens logiques entre les moniteurs et les composants qu'ils contrôlent
  - **Informations temporelles** : la durée et la corrélation temporelle des moniteurs dont l'état est anormal
  - **Informations de confiance statistiques** : la probabilité que le moniteur soit réellement dans un état anormal, tel que la base de référence l'a appris au fil du temps

  Les principaux atouts de nos algorithmes de détection sont les suivants :
  - **Diminution du désordre** : une méthode automatique de regroupement des mesures qui n'ont pas respecté leur base de référence est fournie à l'aide des informations temporelles et topologiques. Cela permet ensuite de

réduire le nombre d'événements qui n'ont pas respecté la base de référence qu'un opérateur devrait examiner sans devoir définir de règles.

- **Diminution du nombre d'événements** : les algorithmes de la solution SHA combinent plusieurs mesures anormales en un seul événement, réduisant le nombre total d'événements présentés à un opérateur. Le point d'entrée de ce type d'événement correspond à plusieurs mesures qui ne respectent pas leurs seuils dynamiques. La solution SHA corrèle alors ces mesures par heure et topologie afin de générer un seul événement permettant à l'opérateur de se concentrer sur le problème réel.
- **Réduction du nombre de fausses alertes** : le nombre de fausses alertes est réduit en calculant l'importance d'une anomalie dans le système à l'aide d'un algorithme statistique. De plus, les anomalies connues qui ont précédemment été marquées comme du bruit seront utilisées pour établir une correspondance avec les anomalies en cours et pour supprimer l'événement d'anomalie.

- **Anomaly DNA Technology — Décodage**

  L'étape qui suit la détection de l'anomalie et sa structure est le décodage de son ADN. Le décodage de l'ADN d'une anomalie est effectué en l'analysant et en le classant selon la topologie (CI et leur structure topologique), les mesures et d'autres informations. Le décodage permet notamment d'obtenir :
  - La séparation des éléments suspects, fournissant ainsi des informations pertinentes. L'identification de l'impact métier à l'aide d'informations relatives à l'entreprise : volume d'utilisateur, contrats de niveau de service (SLA) et zones géographiques concernées, permettant ainsi de hiérarchiser l'anomalie selon l'impact
  - L'identification des changements liés, pouvant avoir modifié le comportement du système

- **Anomaly DNA Technology — Correspondance**

  Une fois la structure de l'ADN de l'anomalie décodée, on effectue la correspondance d'une anomalie actuelle avec des anomalies passées. Cette correspondance est réalisée à l'aide d'un algorithme de similitude de graphique unique, qui compare les structures d'anomalie extraites, permettant ainsi d'établir une correspondance entre les anomalies qui étaient détectées sur différents services avec une architecture semblable. Les avantages de cette correspondance sont les suivants :
  - Elle permet de réutiliser les solutions trouvées dans les événements passés
  - Elle établit une correspondance avec les anomalies des problèmes connus qui doivent encore être résolus, réduisant ainsi le besoin en nouvelles recherches
  - Elle réduit le nombre de fausses alarmes lorsque l'anomalie similaire passée a été classée comme une structure d'ADN bruyante, par exemple une anomalie qui est causée par des actions de maintenance normales sur le service

- **Base de connaissances d'Anomaly DNA**

  Lorsque la base de connaissances des anomalies passées et de leurs résolutions est collectée, l'utilisation des méthodes d'extraction de données avancées permet d'analyser et de générer la relation entre toutes les anomalies, créant ainsi une carte de l'ensemble de la base de connaissances d'Anomaly DNA. Notre algorithme de correspondance de l'ADN des anomalies définit l'espace de mesure requis pour les méthodes d'extraction de données, comme le regroupement et la classification. Elles sont appliquées afin d'offrir les avantages suivants :
  - Résolution proactive des problèmes : identification des problèmes récurrents via la classification de l'ADN des anomalies en types de problème et de résolution, réduisant à l'avenir la durée du diagnostic et de la résolution de ces types
  - Utilisation des connaissances recueillies à partir de différents services qui présentent un comportement semblable.

Fonctionnalités du produit

Basée sur le modèle HP RtSM, la solution HP SHA analyse les tendances et les normes d'historique des applications et de l'infrastructure, puis compare ces données aux mesures de performance en temps réel. L'utilisation d'un modèle RtSM est cruciale pour votre environnement dynamique, afin de pouvoir effectuer les tâches suivantes :

- Corréler les anomalies avec les modifications de la topologie et les problèmes antérieurs ;
- Comprendre l'impact métier de chaque problème et hiérarchiser la résolution ;
- Identifier les éléments suspects du problème et utiliser cette connaissance afin d'empêcher l'apparition de problèmes semblables à l'avenir.

La solution SHA capture automatiquement les seuils dynamiques de votre environnement. Ainsi, il est inutile de demander à des employés de définir et de gérer les seuils statiques. La solution SHA fonctionne sur les mesures provenant des sources de données BSM suivantes :

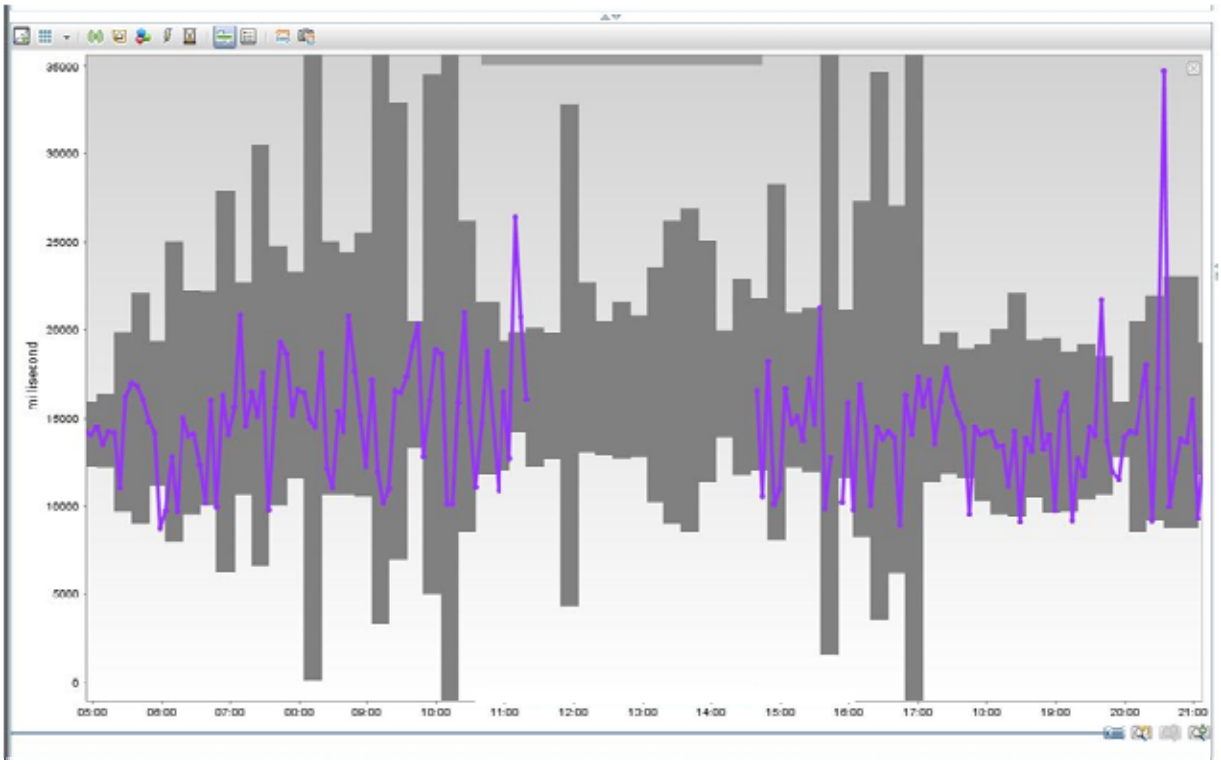
- HP Business Process Monitor
- HP Diagnostics
- HP Network Node Manager i
- HP Operations Manager, Performance Agent
- HP Real User Monitor
- HP SiteScope

La solution SHA identifie les anomalies selon un comportement de mesure anormal lié au modèle RtSM. Elle définit un indice de performance clé et génère un événement dans le contexte qui permet d'identifier la priorité métier concernant ce problème. De plus, elle utilise la technologie Anomaly DNA, pour analyser la conception structurelle d'une anomalie et la comparer à l'ADN connu des autres anomalies. Les correspondances offrent des solutions de résolution connues sans autre enquête, alors que les correspondances qui sont marquées comme bruit sont supprimées. En cas d'anomalies liées à un service spécifique, vous pouvez consulter les contrats de niveau de service pour connaître l'impact potentiel de ces anomalies. Pour finir, la solution SHA comprend les fonctions de résolution du produit HP Closed Loop Incident Process (CLIP) et offre une intégration directe avec HP Operations Orchestration. Vous pouvez par exemple fusionner les analyses et l'automatisation afin de résoudre rapidement les problèmes. Lorsque la solution SHA envoie un événement dans OMi, un opérateur peut prendre des mesures avant que le service soit réduit avec le processus CLIP. Cette résolution rapide simplifie les complexités des environnements de la virtualisation, du cloud et de l'informatique mobile.

Mise en route avec zéro configuration et zéro maintenance

Une fois que vous avez installé le produit et sélectionné les applications que vous voulez contrôler et la solution SHA commence alors à collecter les données et à capturer le comportement de votre système. La solution SHA recueille les données des applications, de l'infrastructure, de la base de données, du réseau et des middlewares, ainsi que des informations sur la topologie à partir du modèle RtSM, et elle appréhende également la base de référence. La base de référence définit le comportement normal d'une mesure individuelle au fil du temps, notamment les caractéristiques périodiques. Le comportement normal d'une mesure peut par exemple comprendre un lundi matin très chargé et un vendredi après-midi très calme.

Figure 3. Exemple de base de référence dynamique (cylindres en gris) avec les données de mesure réelles en violet.

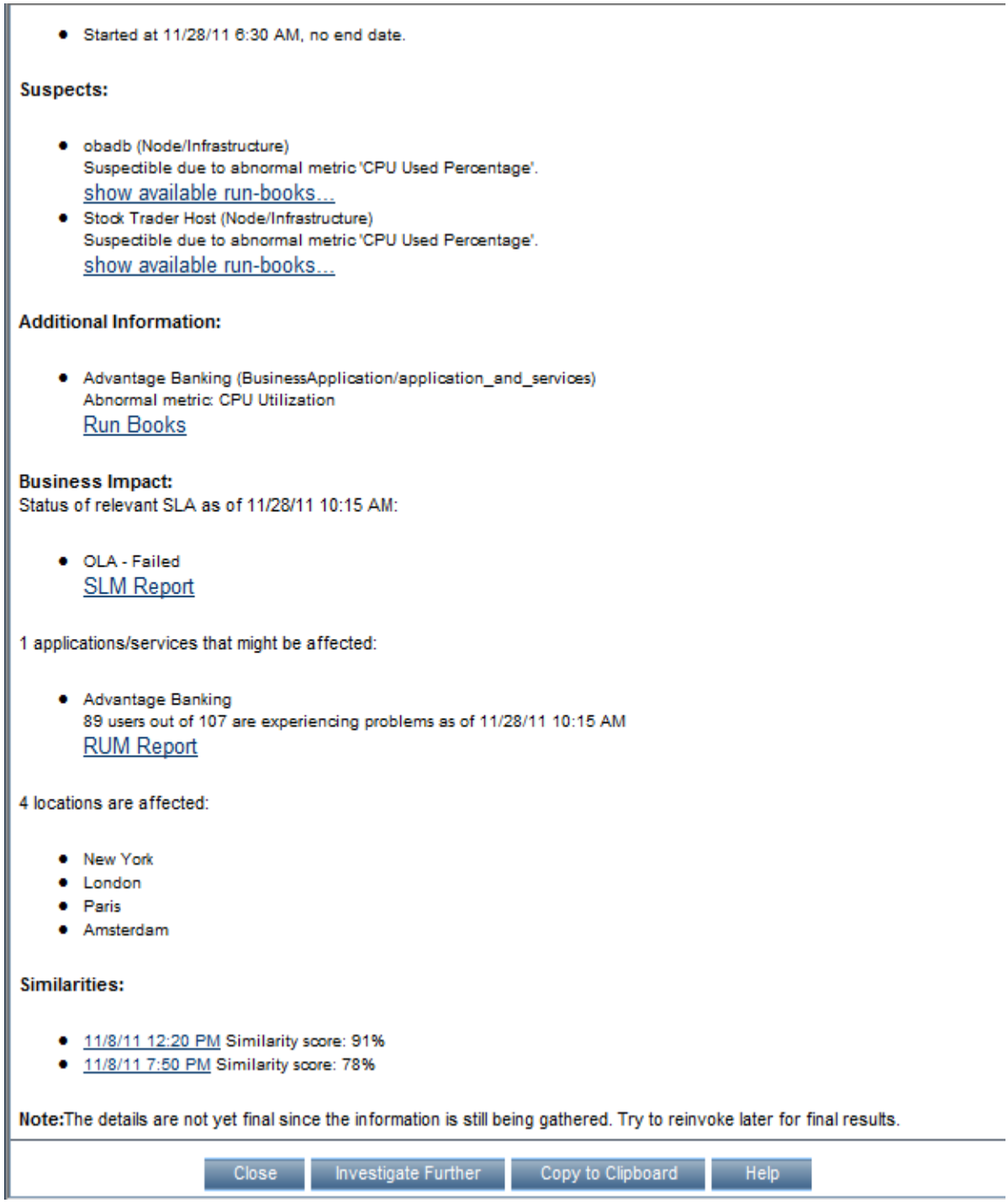


Une fois que vous avez défini les bases de référence dynamiques de toutes les mesures d'application, le moteur RAD de la solution SHA commence à rechercher des anomalies dans le comportement de l'application. Le point d'entrée dans le moteur RAD correspond à un non-respect de la base de référence, indiquant qu'une mesure présente un comportement anormal. Pour définir une anomalie, le moteur RAD prend les informations sur la mesure anormale recueillies à partir de toutes les mesures contrôlées, puis les associe avec les informations sur la topologie du modèle RtSM afin de déterminer s'il existe plusieurs écarts issus de différentes mesures et affectant le même service. Si une anomalie est détectée, un événement est généré et envoyé au sous-système d'événements. De plus, lorsqu'une anomalie est détectée, la solution SHA capture automatiquement la topologie actuelle des CI impliqués dans l'événement. Cela permet de comprendre la topologie telle qu'elle était au moment de l'anomalie, une information particulièrement utile lors de l'examen des anomalies qui se sont produites pendant la nuit ou lorsqu'il n'y avait aucun opérateur d'astreinte pour résoudre les problèmes. La solution SHA collecte et présente également les modifications trouvées pour les CI concernés de façon à ce que les informations puissent être utilisées dans le cadre de l'analyse de la cause première. Cette corrélation se traduit par une résolution plus rapide des problèmes et une diminution du délai moyen de réparation (MTTR).

Lorsque la solution SHA détecte une anomalie dans le comportement de l'application, elle modifie le statut de l'indicateur de performance clé de la santé prédictive et déclenche un événement qui est envoyé au navigateur d'événements BSM. Vous pouvez commencer à descendre dans la hiérarchie à partir de ce point, puis isoler le problème et comprendre son impact métier.

La solution SHA ouvre une page soulignant les anomalies et contenant tout ce que vous avez besoin de savoir sur le problème et son impact métier, ainsi que des fonctions d'isolement avancées si vous devez descendre dans la hiérarchie pour effectuer des recherches complémentaires.

Figure 4. Une page récapitulant les anomalies



En haut de la figure 4 ("Une page récapitulant les anomalies"), vous pouvez trouver la "liste des éléments suspects". Les éléments suspects sont des CI (applications, transactions, éléments d'infrastructure) que la solution SHA a détectés comme étant la cause possible de l'anomalie. Les éléments suspects peuvent être les CI dont les mesures n'ont pas respecté la base de référence, des modèles d'anomalie qui étaient auparavant identifiés par l'utilisateur comme étant anormaux, mais aussi les CI dont les vérifications ont échoué avec l'outil de vérification fourni par l'utilisateur.

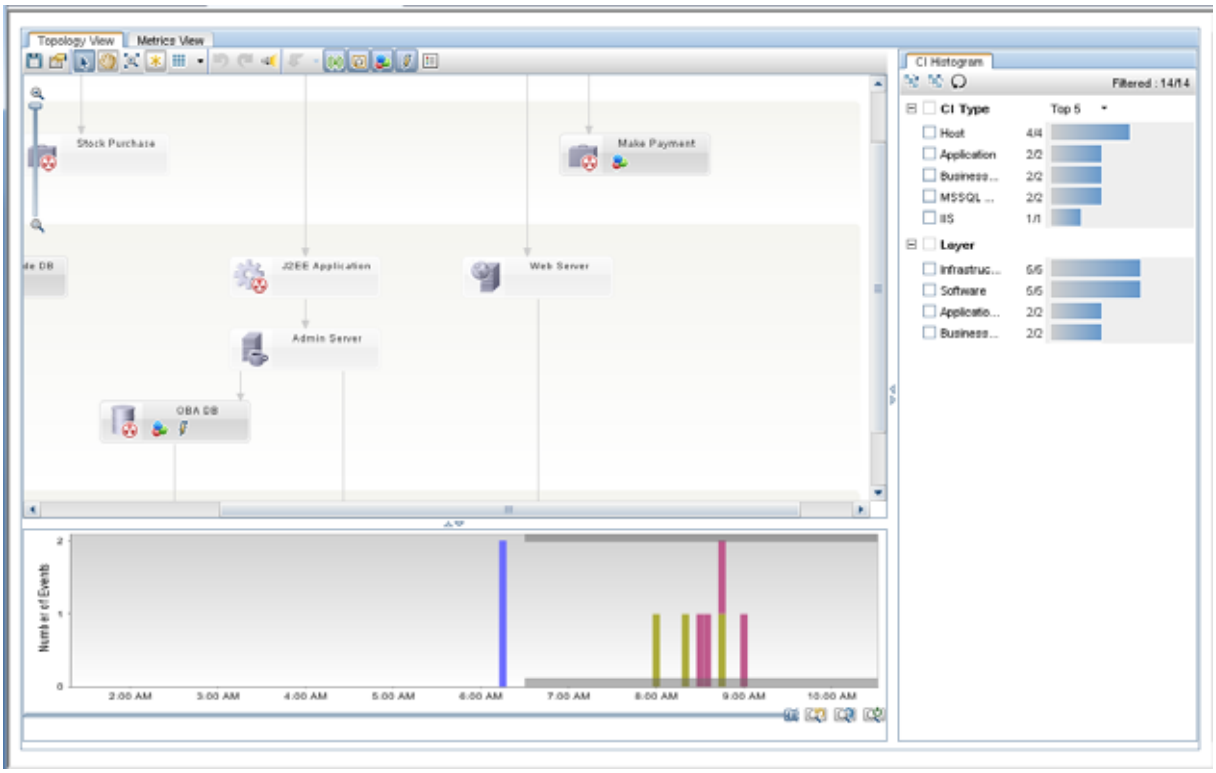
La page récapitulative offre également une vue de l'impact métier de l'anomalie en présentant les contrats de niveau de service qui n'ont pas été respectés à cause de l'anomalie, les services et les applications qui ont été touchés, ainsi qu'une présentation des sites impactés. La solution SHA offre également d'exécuter des rapports pertinents afin de descendre dans la hiérarchie pour avoir une meilleure vue du problème. La section des anomalies similaires est

générée à l'aide de la technologie Anomaly DNA. Elle permet de mieux maîtriser l'occurrence du problème en affichant une liste de modèles semblables, ainsi que des informations supplémentaires sur leur gestion.

La solution SHA fournit une enquête sur le problème et un outil d'isolement permettant de descendre dans la hiérarchie de l'anomalie et d'isoler une cause première possible du problème avec l'interface utilisateur Vue Expertise technique (SME). L'outil d'investigation vous permet de "voyager dans le temps" au sein de l'anomalie afin d'avoir une vue détaillée de la tournure des événements qui ont été à l'origine du problème tel qu'il est reflété dans la topologie de l'application.

La figure ci-dessous montre un exemple d'anomalie et sa tournure d'événements au fil du temps.

Figure 5. Interface utilisateur Vue Expertise technique (SME) montrant la topologie d'une anomalie

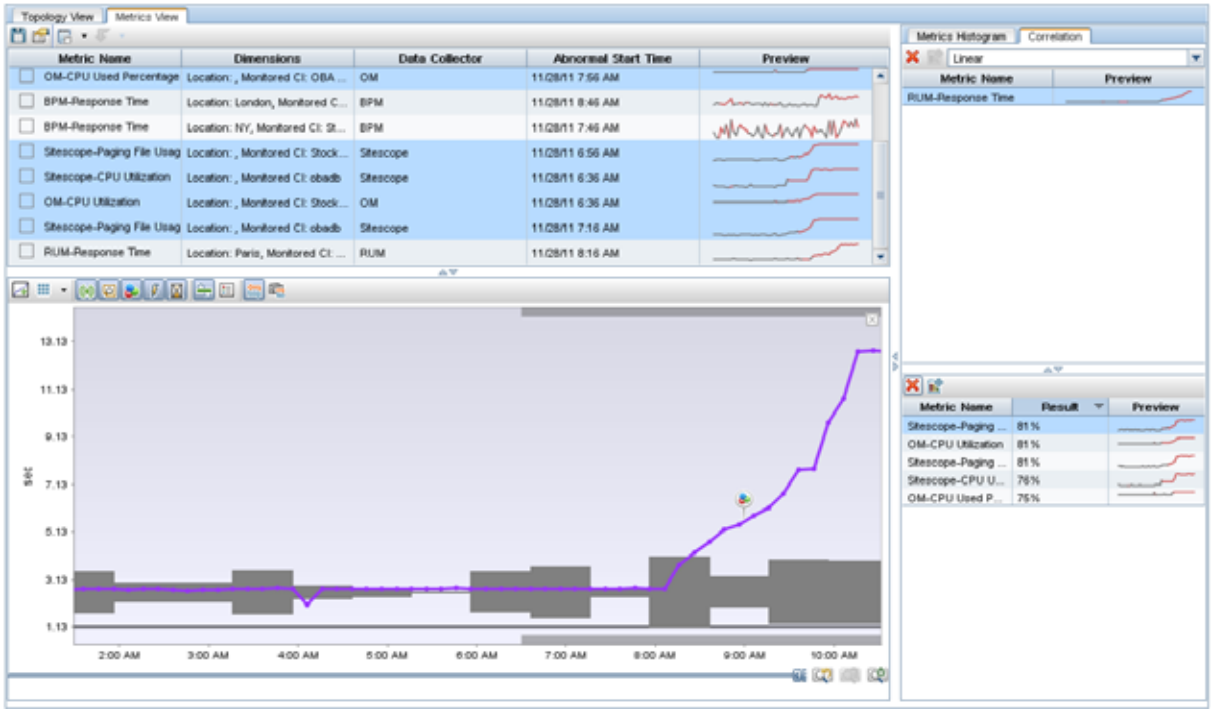


La partie inférieure de l'écran montre les événements du système, tels qu'ils se sont produits et ont été capturés par la solution SHA au fil du temps, avant et pendant l'anomalie.

- A 06:15, SHA a enregistré une modification détectée dans le système.
- A 06:30, SHA a déclenché une anomalie. Cela signifie que la solution SHA a détecté des mesures anormales qui n'ont pas respecté sa base de référence - **avant** que SiteScope et OM, qui surveillaient le système, la découvre. A cet instant précis, la solution SHA **a déjà déclenché un événement qui a été envoyé à l'équipe en charge de l'exploitation**.
- Entre 08:00 et 08:20, SiteScope et OM ont déclenché des événements sur l'utilisation élevée du processeur. La raison pour laquelle SiteScope et OM ont détecté le problème **après la solution SHA**, c'est que leurs seuils étaient définis à un niveau supérieur par rapport à la base de référence dynamique de SHA et ce, afin de réduire le bruit et les fausses alertes positives.
- A 8:30, le premier utilisateur réel a rencontré un problème de performance et a ouvert un incident.

Comme vous pouvez le voir, la solution SHA a détecté le problème et émis une alerte **deux heures à l'avance** et avant que l'un des utilisateurs s'en plaignent, tout en fournissant à l'équipe en charge de l'exploitation un avertissement afin de le gérer et le résoudre.
La solution SHA vous offre un outil puissant permettant de corréler les mesures et de trouver celle qui peut être la cause première du problème dans votre système.

Figure 6. Vue des mesures SHA appartenant à l'interface utilisateur SME



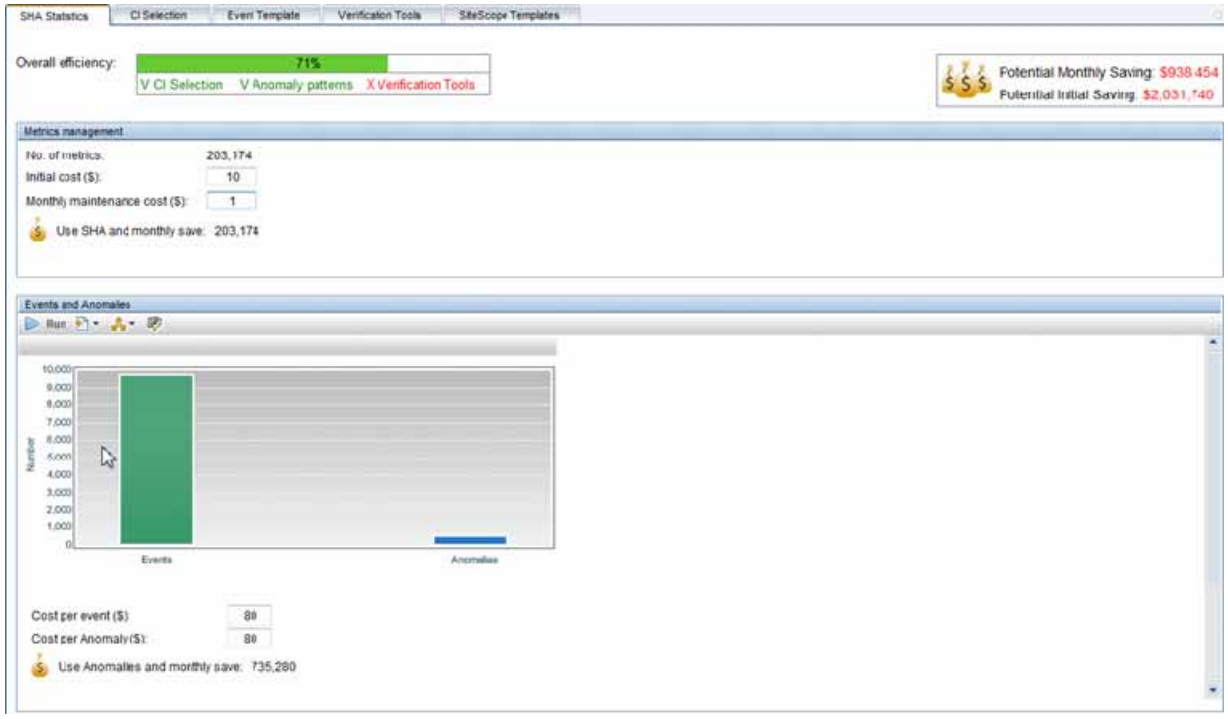
La vue des mesures vous permet de prévisualiser les mesures de votre application telles qu'elles ont été capturées dans le délai de l'anomalie dans "l'enveloppe" de leur base de référence. Elle vous permet également de trouver la mesure qui était la cause première du problème en la corrélant aux autres mesures relatives au même service à l'aide d'algorithmes statistiques complexes.

Dans cet exemple, l'utilisateur a décidé de corréler la mesure Real User Monitor (RUM) avec toutes les autres mesures. La raison pour laquelle cette mesure a été choisie, c'est qu'elle représente le mieux le temps de réponse réel auquel sont soumis les utilisateurs réels lorsqu'ils utilisent l'application. Les autres mesures sont des composants d'infrastructure et de middleware, et la vue des mesures offre un mécanisme de type pointer-cliquer afin de présenter une corrélation entre les mesures et un temps de réponse lent. La mesure qui a obtenu la valeur de corrélation la plus élevée (81 %) était "Sitescope_paging File Usage", qui indique que la cause première est probablement une allocation de mémoire insuffisante.

Retour sur investissement

La solution SHA calcule un retour sur investissement (ROI) à l'aide des informations recueillies à partir de l'environnement de déploiement. La section sur la gestion des mesures étudie le retour sur investissement en réduisant les équipes responsables de l'administration chargées de définir et de gérer les seuils avec les seuils dynamiques autodidactes que la solution SHA fournit. La section sur les événements et les anomalies étudie le retour sur investissement depuis une perspective de réduction du nombre d'événements, comparant le flux d'événements OMi actuel aux événements d'anomalie générés à partir de la solution SHA. Ces informations sont reprises dans l'efficacité globale.

Figure 7. Vue du retour sur investissement de la solution SHA



Conclusion

La solution SHA est un outil d'analyse prédictive d'exécution de future génération, qui peut anticiper les problèmes informatiques avant qu'ils se produisent en analysant le comportement de service anormal et en alertant les responsables informatiques de la dégradation réelle du service avant que ce problème n'ait des conséquences sur le business. La solution SHA offre une intégration étroite avec les solutions HP BSM pour la résolution des événements afin de réduire le délai moyen de réparation (MTTR).

De plus, la solution SHA est simple d'utilisation et nécessite un minimum de configuration et de paramètres. Grâce à la solution SHA, vous n'avez plus à gérer vos seuils de surveillance, car elle capture en permanence le comportement de vos applications et les ajuste en conséquence. Les événements étant de moins en moins nombreux (chacun d'entre eux représentant un problème réel) et SHA se focalisant sur la root cause, le MTTR de vos applications s'en trouve fortement réduit. Optimisée par le modèle HP RtSM dynamique, SHA aide les équipes en charge de l'exploitation à identifier les problèmes potentiels sur la topologie et les services, mais aussi à les résoudre avant que les utilisateurs finaux ne soient impactés.

La solution HP SHA représente la nouvelle ère de l'analyse dans l'IT. Pour plus d'informations, consultez www.hp.com/go/sha.

4AA3-8672FRE, créé en décembre 2011