HP Business Service Management

Für Windows ®- und Linux-Betriebssysteme

Softwareversion: 9.22

Operations Manager i-Konzepthandbuch

Datum der Dokumentveröffentlichung: Mai 2013

Datum des Software-Release: Mai 2013

Rechtliche Hinweise

Garantie

Die Garantiebedingungen für Produkte und Services von HP sind in der Garantieerklärung festgelegt, die diesen Produkten und Services beiliegt. Keine der folgenden Aussagen kann als zusätzliche Garantie interpretiert werden. HP haftet nicht für technische oder redaktionelle Fehler oder Auslassungen.

Die hierin enthaltenen Informationen können ohne vorherige Ankündigung geändert werden.

Eingeschränkte Rechte

Vertrauliche Computersoftware. Gültige Lizenz von HP für den Besitz, Gebrauch oder die Anfertigung von Kopien erforderlich. Entspricht FAR 12.211 und 12.212. Kommerzielle Computersoftware, Computersoftwaredokumentation und technische Daten für kommerzielle Komponenten werden an die U.S.-Regierung per Standardlizenz lizenziert.

Copyright-Hinweis

© Copyright 2008-2013 Hewlett-Packard Development Company, L.P.

Markenhinweise

Adobe® ist eine Marke von Adobe Systems Incorporated.

Microsoft® und Windows® sind in den USA eingetragene Marken der Microsoft Corporation.

UNIX® ist eine eingetragene Marke von The Open Group.

Aktualisierte Dokumentation

Auf der Titelseite dieses Dokuments befinden sich die folgenden identifizierenden Informationen:

- Software-Versionsnummer, die Auskunft über die Version der Software gibt.
- Datum der Dokumentveröffentlichung, das bei jeder Änderung des Dokuments ebenfalls aktualisiert wird.
- Datum des Software-Release, das angibt, wann diese Version der Software veröffentlicht wurde.

Unter der unten angegebenen Internetadresse können Sie überprüfen, ob neue Updates verfügbar sind, und sicherstellen, dass Sie mit der neuesten Version eines Dokuments arbeiten:

http://h20230.www2.hp.com/selfsolve/manuals

Für die Anmeldung an dieser Website benötigen Sie einen HP Passport. Hier können Sie sich für eine HP Passport-ID registrieren:

http://h20229.www2.hp.com/passport-registration.html

Alternativ können Sie auf den Link **New user registration** (Neue Benutzer registrieren) auf der HP Passport-Anmeldeseite klicken.

Wenn Sie sich beim Support-Service eines bestimmten Produkts registrieren, erhalten Sie ebenfalls aktualisierte Softwareversionen und überarbeitete Ausgaben der zugehörigen Dokumente. Weitere Informationen erhalten Sie bei Ihrem HP-Kundenbetreuer.

Support

Besuchen Sie die HP Software Support Online-Website von HP unter:

http://www.hp.com/go/hpsoftwaresupport

Auf dieser Website finden Sie Kontaktinformationen und Details zu Produkten, Services und Support-Leistungen von HP Software.

Der Online-Support von HP Software bietet Kunden mit Hilfe interaktiver technischer Support-Werkzeuge die Möglichkeit, ihre Probleme intern zu lösen. Als Valued Support Customer können Sie die Support-Website für folgende Aufgaben nutzen:

- Suchen nach interessanten Wissensdokumenten
- Absenden und Verfolgen von Support-Fällen und Erweiterungsanforderungen
- Herunterladen von Software-Patches
- Verwalten von Support-Verträgen
- Nachschlagen von HP-Support-Kontakten
- Einsehen von Informationen über verfügbare Services
- Führen von Diskussionen mit anderen Softwarekunden
- Suchen und Registrieren für Softwareschulungen

Für die meisten Support-Bereiche müssen Sie sich als Benutzer mit einem HP Passport registrieren und anmelden. In vielen Fällen ist zudem ein Support-Vertrag erforderlich. Hier können Sie sich für eine HP Passport-ID registrieren:

http://h20229.www2.hp.com/passport-registration.html

Weitere Informationen zu Zugriffsebenen finden Sie unter:

http://h20230.www2.hp.com/new_access_levels.jsp

Inhalt

Willkommen

Dieses Handbuch ist eine Einführung zu HP Business Service Management (BSM) Operationenverwaltung und dient der Beschreibung der wichtigsten Konzepte, die dieser umfassenden Ereignis- und Leistungsmanagementsoftware als einer Komponente der HP Business Service Management-Lösung (BSM) zugrunde liegen.

Hinweis: Die BSM-Operationenverwaltung ist mit einer HP Business Service Management-Bereitstellung (BSM) mit einer aktiven Operations Manager *i*-Lizenz OMi verfügbar (siehe "Einführung in die BSM-Operationenverwaltung" auf Seite 9).

Weitere Informationen zur Bereitstellung von HP Business Service Management finden Sie im *HP Business Service Management Deployment Guide*.

Aufbau dieses Handbuchs

Dieses Handbuch enthält die folgenden Informationen:

- "Einführung in die BSM-Operationenverwaltung" auf Seite 9:

  Eine allgemeine Übersicht über die wichtigsten Funktionen veranschaulicht, wie Sie die BSM-Operationenverwaltung nutzen können, um die Leistung, Verfügbarkeit und Effizienz Ihre IT-Umgebung zu verbessern.

- "Workflow des Operators" auf Seite 33:

  Eine Beschreibung, wie ein normaler Tag für Dave, den Operator im Bereich IT-Betrieb, aussieht und wie er die Ereignisverwaltung nutzt, um seine täglichen Aufgaben nach Prioritäten zu ordnen.

- "Workflow des Entwicklers von Überwachungslösungen" auf Seite 39:

  Eine Beschreibung, wie die Rolle von Mike, einem Entwickler von Überwachungslösungen im Bereich IT-Betrieb, aussieht und wie er eine neue Applikation überwacht.

- "Workflow des Systemadministrators im Bereich IT-Betrieb" auf Seite 43:

  Eine Beschreibung, wie die Rolle von Matthew aussieht und wie er die Umgebung der BSM-Operationenverwaltung überwacht und die Betriebsinfrastruktur so konfiguriert, dass alle Applikationen und Server in seiner Domäne integriert werden.

- "Workflow der Applikationsspezialistin" auf Seite 47:

  Eine Beschreibung, wie die Rolle von Alice aussieht und wie sie generische Überwachungslösungen für alle Applikationen und Server in ihrem Bereich konfiguriert.

Wer dieses Handbuch lesen sollte

Dieses Handbuch sollten Sie lesen, wenn Sie einer der folgenden Benutzer sind:

- Operator im Bereich IT-Betrieb
- Fachexperte für Datenbanken, Exchange, SAP oder sonstiger Fachexperte, der die Überwachungsszenarios für diese Unternehmensapplikationen gestaltet
- Entwickler von Überwachungslösungen im Bereich IT-Betrieb
- Systemadministrator im Bereich IT-Betrieb
- Applikationsadministrator im Bereich IT-Betrieb
- Wenn Sie einer dieser Benutzer sind, sind Sie sicher mit BSM und den grundlegenden Konzepten der Überwachung und des Managements in Unternehmen vertraut.

Einführung in die BSM-Operationenverwaltung

In diesem Kapitel finden Sie einen allgemeinen Überblick über die BSM-Operationenverwaltung und erfahren, wie Sie damit die Effizienz Ihrer IT-Services und IT-Infrastruktur verbessern können.

Dieses Kapitel enthält eine Übersicht über die Architektur, zeigt, wie die BSM-Operationenverwaltung in eine HP Business Service Management-Lösung (BSM-Lösung) passt, und beschreibt die zugrunde liegenden Konzepte.

Das Kapitel ist wie folgt strukturiert:

Lizenzstruktur

Die BSM-Operationenverwaltung ist in einer Bereitstellung von HP Business Service Management (BSM) mit aktiver Operations Manager-Lizenz *i*-Lizenz (OMi) verfügbar.

Weitere Informationen zur Bereitstellung finden Sie im HP Business Service Management Deployment Guide.

Die Lizenzstruktur von Operations Manager *i* (OMi) stellt sich wie folgt dar:

- **Ereignisverwaltung-Foundation**

  Die Lizenz für Ereignisverwaltung-Foundation ist für die Funktionalität der BSM-Operationenverwaltung erforderlich.

- **Topologiebasierte Ereigniskorrelation**

  Die Lizenz für topologiebasierte Ereigniskorrelation wird für TBEC-Funktionen benötigt. Diese Lizenz baut auf der Ereignisverwaltung-Foundation-Lizenz auf.

- **Ziel-Konnektor**

  Für jedes System, das mit einer Managementlösung eines Drittanbieters verwaltet wird, wobei Ereignisse in der BSM-Operationenverwaltung zusammengefasst werden, ist eine Ziel-

Konnektor-Lizenz erforderlich. Diese Lizenz baut auf der Ereignisverwaltung-Foundation-Lizenz auf.

- **Monitoring Automation**

  Für die Überwachung von Applikationen direkt aus HP Operations Manager i ist eine Monitoring Automation-Lizenz erforderlich. Monitoring Automation wird in zwei Varianten angeboten:

  - *Monitoring Automation für Server*

    Monitoring Automation für Server konzentriert sich auf virtuelle und physische Systeme und serverorentierte Anwendungen. Die OMi-Ereignisverwaltung-Foundation umfasst Monitoring Automation für Server.

  - *HP Monitoring Automation for Composite Applications*

    HP Monitoring Automation for Composite Applications bietet erweiterten Funktionen speziell für dynamische Rechenzentren, wie z. B. die topologiebasierte Überwachungskonfiguration für komplexe, mehrstufige Applikationen, wodurch die Überwachungskonfiguration automatisch angepasst wird, wenn Applikationsinstanzen oder -parameter an Geschäfts- oder Umgebungsanforderungen angepasst werden. Eine Lizenz für HP Monitoring Automation für Composite Applications kann als Add-On zur HP Operations Manager i-Lösungsfamilie erworben werden.

- Die BSM-Operationenverwaltung bildet die Basis für die Ereignisverwaltung für eine komplette BSM-Überwachungslösung. Als Operations Bridge konsolidiert sie die gesamte Überwachung der IT-Infrastruktur in einer zentralen Ereigniskonsole und setzt die Ereignisse mit den IT-Services in Beziehung, die von dieser Infrastruktur abhängig sind. Benutzern steht damit ein einheitlich strukturiertes Modell zur Ereignisverwaltung zur Verfügung, dass auf Business Service Management und das IT-Infrastrukturmanagement dieselben Prozesse anwendet.

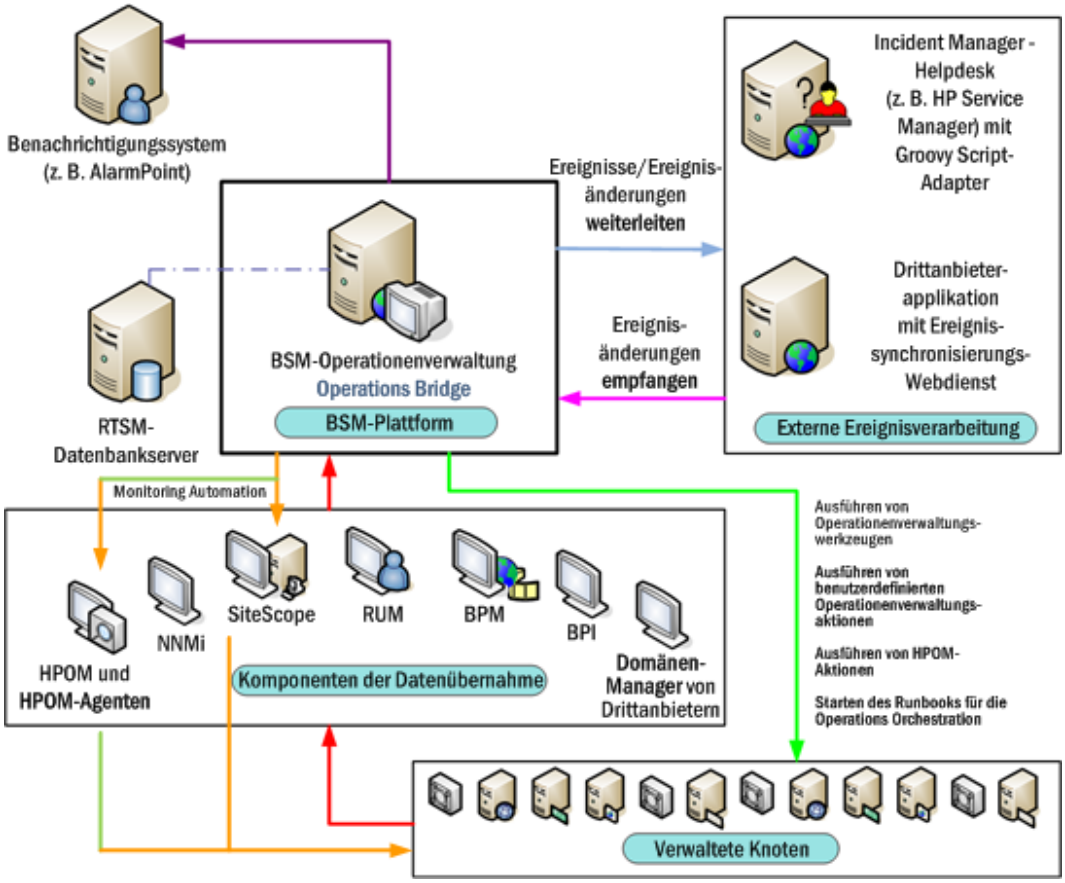
Operations Bridge für eine vollständige BSM-Lösung

Die BSM-Operationenverwaltung bildet die Basis für die Ereignisverwaltung für eine komplette BSM-Überwachungslösung. Als Operations Bridge konsolidiert sie die gesamte Überwachung der IT-Infrastruktur in einer zentralen Ereigniskonsole und setzt die Ereignisse mit den IT-Services in Beziehung, die von dieser Infrastruktur abhängig sind. Benutzern steht damit ein einheitlich strukturiertes Modell zur Ereignisverwaltung zur Verfügung, dass auf Business Service Management und das IT-Infrastrukturmanagement dieselben Prozesse anwendet.

Die BSM-Operationenverwaltung verknüpft die Infrastrukturverwaltung mit dem Applikations- und dem Business-Service-Management. Sie kombiniert Ereignisse von HP Business Service Management-Komponenten, wie Business Process Monitor (BPM), Real User Monitor (RUM) und Service Level Management (SLM), mit Ereignissen aus Operationenverwaltungs-Komponenten der BSM-Lösung, wie HP Operations Manager (HPOM) und HP Network Node Manager i (NNMi). Dies ermöglicht die Verfolgung aller Ereignisse, die in Ihrer überwachten Umgebung auftreten.

Abbildung 1 auf der nächsten Seite zeigt ein Beispiel für eine typische Bereitstellung, bei der die BSM-Operationenverwaltung als Operations Bridge in einer BSM-Lösung fungiert. Die BSM-Operationenverwaltung ermöglicht die automatisierte Überwachung und Integration von mehreren externen Applikationen und wird in der BSM-Plattform unter Verwendung der gemeinsamen RTSM-Datenbank (Run-Time Service Model) ausgeführt.

Abbildung 1 – Operations Bridge in einer BSM-Lösung



Die gemeinsame Nutzung des RTSM mit anderen BSM-Applikationen bedeutet, dass immer ein direkter Zugriff auf die neuesten Daten im RTSM möglich ist. Dadurch entsteht für Systemadministratoren im Bereich IT-Betrieb kein zusätzlicher Aufwand bei der Verwaltung der Topologiedaten im RTSM.

Alle Ereignis- und Leistungsmanagementdaten von Servern, Netzwerken, Applikationen, Speichern und anderen IT-Silos in Ihrer Infrastruktur werden in einem einzigen Ereignisstrom in einer erweiterten, zentralen Ereigniskonsole konsolidiert. Auf der Konsole werden Warnungen aus der Überwachung für die Operatoren des zuständigen Teams angezeigt.

Probleme in Ihrer verteilten IT-Umgebung können Sie schnell erkennen, überwachen und beheben und entsprechende Reports erstellen. All dies ermöglicht es Ihnen, die Leistung und Verfügbarkeit der Infrastruktur und Services in Ihrer überwachten Umgebung zu verbessern und damit die Effizienz und Produktivität Ihres Unternehmens zu erhöhen. Die BSM-Operationenverwaltung hilft Ihnen, ereignisbezogene Probleme zu finden und zu lösen, bevor sich die Qualität der Geschäftsservices verschlechtert. Mit den bereitgestellten Werkzeugen können die Operatoren Probleme lösen, ohne einen Fachexperten hinzuziehen zu müssen. Dadurch können sich die Fachexperten mehr auf strategische Aktivitäten konzentrieren.

Datenübernahme aus mehreren Quellen

Wie Abbildung 1 auf der vorherigen Seite zeigt, werden Ereignisse ungeachtet dessen, woher sie stammen, auf einheitliche Art und Weise verarbeitet und verwaltet.

Beispiele für Ereignisquellen:

- BSM-Komponenten:
  BSM-Warnungen (CI-Status-Warnungen, SLA-Warnungen und ereignisbasierte Warnungen) können ebenfalls Ereignisse in der BSM-Operationenverwaltung generieren. Zum Beispiel können Operatoren Ereignisse sammeln, anzeigen, korrelieren und verwalten, die aus ereignisbasierten Warnungen von EUM-Komponenten generiert werden. Beachten Sie, dass Warnungen, die von einer EUM-Komponente, zum Beispiel BPM, weitergeleitet wurden, nicht zurück synchronisiert werden.
- BSM-Komponenten:
  - HP Operations Manager for UNIX (HPOM for UNIX) mit einem Operations Manager-Server auf einer HP-UX-, SPARC Solaris- oder x64 RHEL-Plattform
  - HP Operations Manager für Windows (HPOM für Windows)
  - HP Network Node Manager i (NNMi)
  - Business Process Monitor (BPM)
  - Real User Monitor (RUM)
  - HP SiteScope
  - HP Systems Insight Manager

  BSM-Warnungen (CI-Status-Warnungen, SLA-Warnungen und ereignisbasierte Warnungen) können ebenfalls Ereignisse in der BSM-Operationenverwaltung generieren. Zum Beispiel können Operatoren Ereignisse sammeln, anzeigen, korrelieren und verwalten, die aus ereignisbasierten Warnungen von EUM-Komponenten generiert werden. Beachten Sie, dass Warnungen, die von einer EUM-Komponente, zum Beispiel BPM, weitergeleitet wurden, nicht zurück synchronisiert werden.
- Managementsoftware von Drittanbietern, die zur Überwachung bestimmter Umgebungen oder spezieller Anforderungen, die von anderen Lösungskomponenten nicht überwacht werden, eingesetzt wird, wie zum Beispiel Microsoft Systems Center Operations Manager oder Oracle Enterprise Manager. Konnektoren zur Integration von Managementsoftware von Drittanbietern, wie zum Beispiel Microsoft SCOM, Nagios und IBM Tivoli, in HP BSM sind auch im HP Live Network-Portal (https://hpln.hp.com) verfügbar.

Konsolidiertes Ereignis- und Leistungsmanagement

Die Operations Bridge ist die Stelle, an der Ereignisse aller Typen aus mehreren Quellen in einer zentralen Konsole konsolidiert werden. In "Perspektiven" erhalten die Operatoren zu den Ereignissen, für die sie verantwortlich sind, Informationen auf unterschiedlichen Ebenen. Zum Beispiel erfolgt die allgemeine Ereignisverarbeitung in der Ereignisperspektive, während die Zustandsperspektive zusätzliche servicezustandsbezogene Informationen zu den Ereignissen bereitstellt. Diese Perspektiven haben den Ereignis-Browser zum Mittelpunkt.

Ereignisinformationen

Ereignisse melden wichtige Geschehnisse in der verwalteten IT-Umgebung. Sie werden durch Domänen-Manager generiert, an die Operationenverwaltung weitergeleitet und dann zugehörigen

CIs (Configuration Items, Konfigurationselementen) im RTSM zugeordnet. Diese Ereignisse werden Operatoren zur Lösung zugewiesen. Im Ereignis-Browser wird den Operatoren eine vollständige Übersicht über alle aktiven Ereignisse angezeigt, die bearbeitet werden müssen. Dort sind Informationen wie der Schweregrad und der Typ des Ereignisses, die Kategorie des Ereignisses, die Ereignisquelle, Ereigniszeit und -ort sowie das betroffene CI zu finden.

Ereignisse durchlaufen einen "Lebenszyklus", bei dem es sich um eine informative Art der Anzeige und Überwachung des Status eines Ereignisses handelt. Der Workflow eines Operators hängt vom Lebenszyklus eines Ereignisses ab. Der Lebenszyklusstatus eines Ereignisses repräsentiert den Fortschritt der Untersuchung des Problems, durch das dieses Ereignis verursacht wurde. Der Operator, der einem Ereignis zugewiesen wurde, öffnet eine Untersuchung und arbeitet daran, eine Lösung für das dem Ereignis zugrunde liegende Problem zu finden. Experten können dann die vorgeschlagene Lösung bewerten, überprüfen, ob das Problem, durch das das Ereignis verursacht wurde, damit gelöst werden kann, und das Ereignis schließen, womit der Lebenszyklus abgeschlossen ist.

Die Operatoren können den Ereignis-Browser entsprechend den Anforderungen ihrer typischen Workflows konfigurieren. Der Inhalt des Ereignis-Browsers wird nach ausgewähltem CI oder anhand der ausgewählten Ansicht gefiltert. Die Operatoren können neue Filter konfigurieren oder vorhandene Filter modifizieren, um die angezeigten Informationen entsprechend ihren Anforderungen zu ändern. Durch Filtern des Inhalts im Ereignis-Browser können sich die Operatoren auf die nützlichen Informationen konzentrieren, zum Beispiel um die Ereignisse mit der höchsten Priorität zu finden und festzustellen, welche dieser Ereignisse zuerst untersucht werden müssen, um die Auswirkungen auf die Geschäftsservices zu minimieren. Sie können auch Benutzer und Gruppen konfigurieren, sodass diese nur die Ereignisse anzeigen können, die nach den Ansichten für diesen Benutzer oder diese Gruppe gefiltert sind.

Sie können Daten-Collectoren von HP oder anderen Anbietern so konfigurieren, dass sie Ereignisse an die BSM-Operationenverwaltung weiterleiten. Ereignisse werden zwischen den Servern synchronisiert. Zum Beispiel synchronisieren die BSM-Operationenverwaltung und HP Operations Manager (HPOM) den Status von Ereignissen und Nachrichten. Wenn ein BSM-Operationenverwaltungs-Operator ein Ereignis schließt, wird automatisch eine Benachrichtigung an HPOM gesendet. Analog wird die BSM-Operationenverwaltung von HPOM über die Bestätigung von Nachrichten benachrichtigt und die BSM-Operationenverwaltung setzt die entsprechenden Ereignisse automatisch auf den neuen Lebenszyklusstatus "Geschlossen".

Die Operatoren können Ereignisse mit zusätzlichen Informationen anreichern, zum Beispiel indem sie zum Ereignis Anmerkungen hinzufügen, um die Problemlösung zu unterstützen oder zu dokumentieren, was bereits unternommen wurde.

Geschlossene Ereignisse werden automatisch in den Browser für geschlossene Ereignisse verschoben. Die Operatoren können dann auf diese Liste der geschlossenen Ereignisse zugreifen und diese Ereignisse als Referenz für die Lösung ähnlicher Probleme verwenden.

Ereignisse, um die sich bestimmte Fachexperten kümmern müssen, können durch die Operations Bridge an die entsprechenden Operatoren weitergeleitet werden. Zum Beispiel kann der Systemadministrator im Bereich IT-Betrieb das System so konfigurieren, dass Benachrichtigungen an Operatoren und Eskalationen an die entsprechenden Helpdesk-Operatoren gesendet werden, die sich auf die Verwaltung von eskalierten Ereignissen und Behebung der zugrunde liegenden Probleme konzentrieren können.

Ereignis-Dashboards

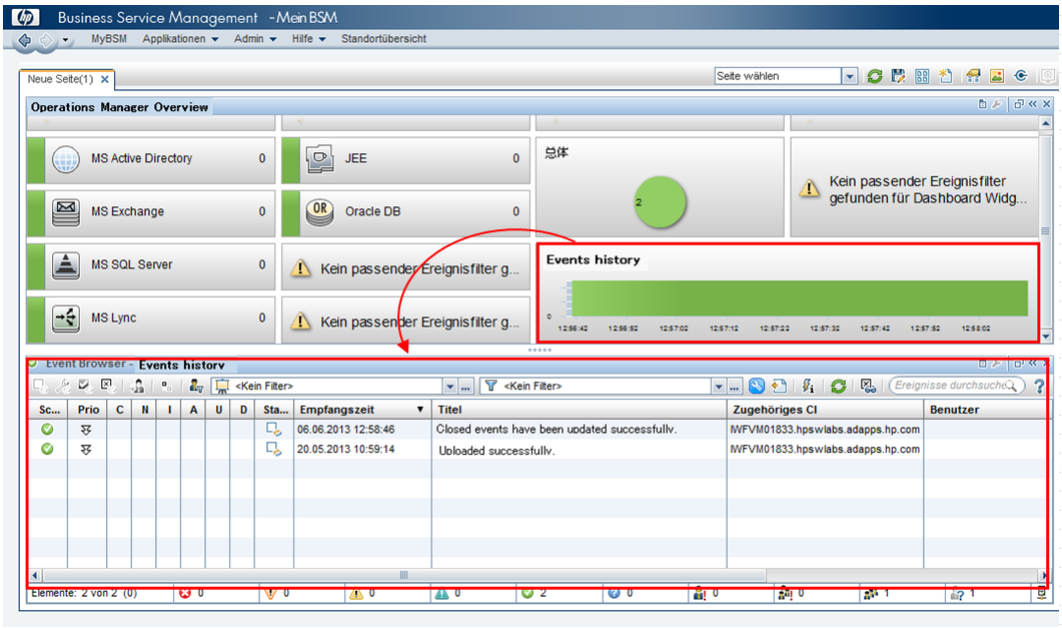
Ereignis-Dashboards (siehe Abbildung 2 unten) bieten Ihnen auf einen Blick eine Übersicht über die Ereignisse aus einer überwachten Umgebung. Sie ermöglichen Ihnen, den Zustand der Umgebung schnell zu erfassen und Bereiche zu identifizieren, die Ihre Aufmerksamkeit erfordern.

Mit Ereignis-Dashboards können Sie:

- sich eine Übersicht über die überwachte Umgebung verschaffen
- einen Ausgangspunkt für tägliche Verwaltungsaufgaben visualisieren
- Ereignisfilter schnell auf den Ereignis-Browser anwenden
- die überwachte Umgebung während der Arbeit an einem Ereignis weiter beobachten

In den Ereignis-Dashboards werden Statusinformationen mithilfe verschiedener Widgets als Bausteine (z. B. Balken- und Kreisdiagramme) dargestellt. Jedes Widget referenziert einen Ereignisfilter, eine Ansicht oder beides und zeigt nur den Status derjenigen Ereignisse an, die den Filterkriterien entsprechen und den CIs in der referenzierten Ansicht zugeordnet sind, was eine Anpassung sehr erleichtert.

Abbildung 2 – Ereignis-Dashboard



Zustandsinformationen

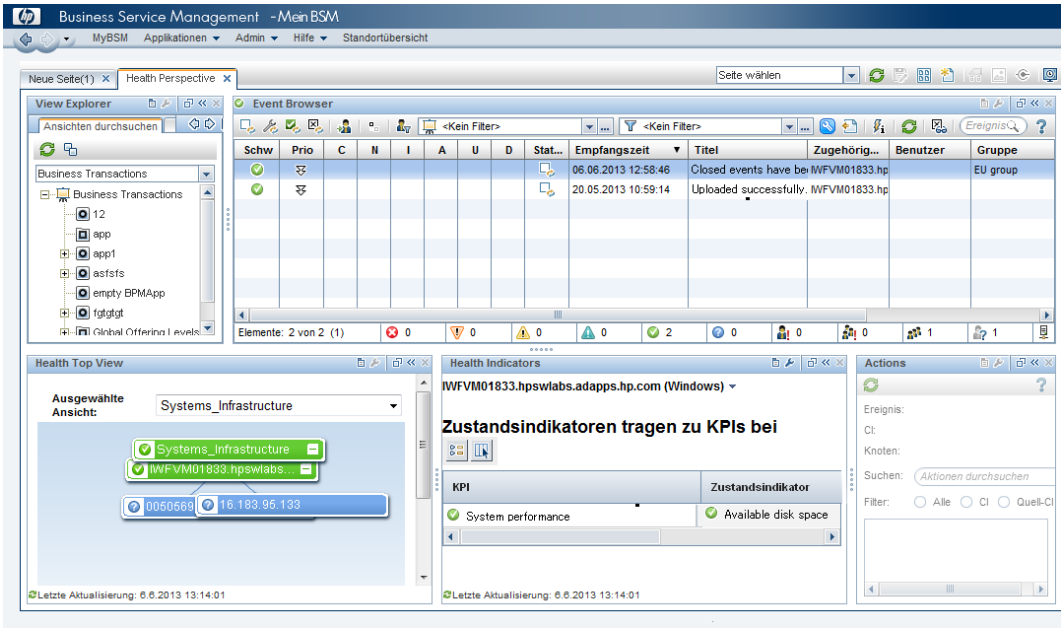
Mit ereignisbasierten Daten können Sie im Ereignis-Browser sehen, welches zugehörige CI durch das Ereignis betroffen ist. Außerdem werden BSM-Zustandsdaten wie Ereignistypindikatoren (ETIs), Zustandsindikatoren (HIs) und zentrale Leistungsindikatoren (KPIs) verwendet, um den Zustand zugehöriger CIs im Kontext der Ereignisse zu evaluieren.

Für jedes Gerät, z. B. einen Server, wird der Schweregrad der Probleme, die in direktem Zusammenhang mit dem Server stehen, erfasst und mit Informationen zu Geräten kombiniert, die dem Server zugeordnet sind. Die kombinierten Daten werden zur Auswertung und Festlegung der

zentralen Leistungsindikatoren, die den Gesamtzustand des Objekts wiedergeben, an Berechnungsregeln übergeben.

Abbildung 3 unten zeigt eine typische Seite mit einer Zustandsperspektive, bei der die Zustandstopologieansicht eine hierarchische Übersicht der Beziehungen zwischen den Objekten, die mit dem Ereignis verknüpft sind, enthält.

Abbildung 3 – Zustandsperspektive mit den Bereichen "Zustandstopologieansicht" und "Zustandsindikatoren"



Sie sehen den Zustand eines Objekts, die verwendeten Geschäftsregeln und KPIs und die Auswirkungen des Zustands des ausgewählten Objekts auf den Zustand zugehöriger CIs. Zum Beispiel kann ein Benutzer auch den Zustand der benachbarten CIs überprüfen. Mit diesen Informationen kann der Benutzer analysieren, auf welche Ereignisse er sich konzentrieren sollte, und die Ereignisverarbeitung priorisieren, um die Verfügbarkeit zu maximieren und die negativen Auswirkungen auf Geschäftsservices zu minimieren. Der Benutzer kann auch bestimmte Ansichten auswählen, damit nur die Ereignisse und CIs angezeigt werden, für die er verantwortlich ist.

Der Benutzer kann eine Komponente auswählen und sieht dann den Status der zugehörigen Zustandsindikatoren und KPIs. So kann zum Beispiel ein Operator den Status des KPI "Verfügbarkeit" für einen bestimmten Server und den Status der zugehörigen Zustandsindikatoren anzeigen lassen.

Korrelieren von Ereignissen

In einer umfangreichen Umgebung besteht eine der größten Herausforderungen darin, wie die große Anzahl an Ereignissen aus den verschiedensten Quellen verwaltet werden soll. Ziel dabei ist es, in dieser Datenflut die Ereignisse zu identifizieren, die signifikante Auswirkungen auf Geschäftsservices haben. Auch, wenn es auch wichtig ist, die Anzahl der angezeigten Ereignisse im Ereignis-Browser zu minimieren, ist es jedoch noch wichtiger, die Ereignisse hervorzuheben, die, wenn sie nicht ordnungsgemäß behandelt werden, Vereinbarungen zum Servicelevel (Service Level Agreements, SLAs) verletzen und Vorfälle in Ihrem Helpdesk-System generieren könnten.

Die Ereigniskorrelation spielt eine wichtige Rolle bei der Aufgabe, das Management von Geschäftsservices und das Management von IT-Infrastrukturen so zu verbinden, dass die Unterbrechung eines Service bis zu einem bestimmten Fehler in der IT-Infrastruktur, von der der Service abhängt, verfolgt werden kann.

Die BSM-Operationenverwaltung korreliert Ereignisse automatisch und verwendet dabei die folgenden Formen der Ereigniskorrelation:

- Unterdrücken doppelter Ereignisse
- Automatisches Schließen zugehöriger Ereignisse
- Stream-basierte Ereigniskorrelation
- Topologiebasierte Ereigniskorrelation

Unterdrücken doppelter Ereignisse

Bei einem neuen Ereignis kann es sich um ein Duplikat eines vorhandenen Ereignisses handeln. Ein einfaches Beispiel wäre, wenn wegen Netzwerkstabilitätsproblemen ein Domänen-Manager einer Quelle ein Ereignis zwei Mal sendet, da er die Bestätigung für die erste Instanz des Ereignisses nicht schnell genug erhalten hat. Neue Ereignisse werden bei Empfang mit vorhandenen Ereignissen vergleichen. Wenn dabei Duplikate gefunden werden, wird das vorhandene Ereignis mit den neuen Informationen (zum Beispiel einer Änderung im Schweregrad) aktualisiert und das neue Ereignis wird ignoriert. Ist die Unterdrückung doppelter Ereignisse aktiviert, bleiben neue Ereignisse, bei denen es sich um Duplikate von vorhandenen Ereignissen handelt, nicht erhalten, sondern das ursprüngliche Ereignis wird aktualisiert.

Das Korrelieren von Ereignissen mit Unterdrückung doppelter Ereignisse hat den Vorteil, dass dabei die Anzahl der angezeigten Ereignisse in der Konsole reduziert wird, ohne dass wichtige Informationen verloren gehen.

Die Unterdrückung doppelter Ereignisse kann zusätzliche Korrelationen des ursprünglichen Ereignisses zur Folge haben (sowohl als Ursache als auch als Symptom). Bei Identifizierung eines Duplikats wird der Zeitstempel für das ursprüngliche Ereignis mit dem Zeitpunkt aktualisiert, an dem das Duplikat empfangen wurde. Das Ereignis wird dann erneut korreliert und kann jetzt mit anderen Ereignissen verknüpft werden, die bei Empfang des ursprünglichen Ereignisses nicht für die Korrelation zur Verfügung standen.

Automatisches Schließen zugehöriger Ereignisse

Ein neues Ereignis kann automatisch ein oder mehrere vorhandene Ereignisse schließen. Wenn ein neues Ereignis empfangen wird, wird eine Suche nach vorhandenen zugehörigen Ereignissen durchgeführt. Einige spezielle Informationen im neuen Ereignis werden verwendet, um es mit vorhandenen Ereignissen zu vergleichen, und wenn sie übereinstimmen, wird das vorhandene Ereignis geschlossen. Diese Art der Ereigniskorrelation ähnelt der "Gut/Schlecht"-Nachrichtenkorrelation in HP Operations Manager.

Als Beispiel soll ein vorhandenes Ereignis dienen, bei dem es sich um eine Benachrichtigung über ein Problem oder eine abnormale Bedingung (ein schlechtes Ereignis) für ein bestimmtes Gerät handelt. Das schlechte Ereignis könnte "`SQL-Abfrageleistung NIEDRIG`" lauten. Nun geht ein neues Ereignis ein, das mit dem vorhandenen zugehörigen Ereignis übereinstimmt und die Benachrichtigung enthält, dass die abnormale Bedingung nicht mehr vorhanden ist (ein gutes Ereignis). Das gute Ereignis könnte "`SQL-Abfrageleistung HOCH`" lauten. Das neue (gute) Ereignis schließt dann das vorhandene (schlechte) zugehörige Ereignis.

In der Ereignishistorie können Sie zugehörige Ereignisse, die automatisch geschlossen wurden, verfolgen.

Stream-basierte Ereigniskorrelation

In der Stream-basierten Ereigniskorrelation (SBEC) werden Regeln und Filter verwendet, um häufig auftretende Ereignisse oder Kombinationen von Ereignissen zu identifizieren. Sie hilft bei der Verarbeitung solcher Ereignisse, in dem die Ereignisse automatisch identifiziert werden, die zurückgehalten oder entfernt werden können oder für die ein neues Ereignis erstellt und den Operatoren angezeigt werden muss.

Folgende Typen von SBEC-Regeln können konfiguriert werden:

- **Wiederholungsregeln:** Häufige Wiederholungen eines Ereignisses können auf ein Problem hinweisen, das geprüft werden muss.
- **Kombinationsregeln:** Eine Kombination aus verschiedenen Ereignissen, die zusammen oder in einer bestimmten Reihenfolge auftreten, weist auf ein Problem hin und erfordert eine spezielle Behandlung.
- **Regeln zu fehlenden Serienereignissen:** Ein regelmäßig auftretendes Ereignis findet nicht statt, z. B. ein reguläres Heartbeat-Ereignis, das nicht wie erwartet eintritt.

Topologiebasierte Ereigniskorrelation

Der Ereignisverwaltungsprozess wird nicht nur durch Konsolidierung der Ereignisse aus allen Quellen in einer zentralen Konsole vereinfacht, sondern auch durch Kategorisierung von Ereignissen mit der topologiebasierten Ereigniskorrelation (TBEC). Dabei werden die Abhängigkeiten zwischen Ereignissen analysiert, um zu ermitteln, ob einige Ereignisse durch andere Ereignisse erklärt werden können. Als Beispiel soll ein Datenbankserver (DB-Server) dienen, der auf einem Server (Server1) ausgeführt wird. Wenn die CPU-Auslastung von Server1 eine dauerhafte Überlastung anzeigt, kann das generierte Ereignis "`SLA für DB-Server nicht erfüllt`" durch das Ursachenereignis "`Server1: CPU dauerhaft überlastet (100 % für mehr als 10 Minuten)`" erklärt werden.

Der Schlüssel besteht darin, die zugrunde liegenden Ursachenereignisse genau zu bestimmen, die für andere Symptomereignisse verantwortlich sind, damit Sie die Auflösung dieser Ursachenereignisse auf der Basis der Auswirkungen auf Ihr Unternehmen priorisieren können.

Wenn zwei Ereignisse gleichzeitig (in einer konfigurierbaren Zeitspanne) auftreten, identifizieren die TBEC-Korrelationsregeln ein Ereignis als Ursache und das andere Ereignis als Symptom. Mit der regelbasierten Ereignisverwaltung können Sie große Mengen ähnlicher (zugehöriger) Symptomereignisse in einem großen Netzwerk verwalten.

Wenn in der überwachten Umgebung ein Ereignis als Kombination aus Ursache und Symptom auftritt, werden die korrelierten Ereignisse im Ereignis-Browser mit einem Flag versehen. Sie können den Ereignis-Browser so konfigurieren, dass das Ursachenereignis und eine separate Übersicht mit allen Symptomereignissen angezeigt werden, sodass Sie Details zum Korrelationsprozess anzeigen und durch die Hierarchie der korrelierten Ereignisse navigieren können.

Ereignisse können auch zwischen mehreren technischen Bereichen (Datenbanken, Hardware, Netzwerke und Webapplikationen) korreliert werden. Dieser umfassende Geltungsbereich ermöglicht Ihnen die Korrelation von Ereignissen, zwischen denen auf den ersten Blick keine Verbindung zu erkennen ist. Die domänenübergreifende Funktionalität erhöht auch die Produktivität, da das Ausmaß der Überschneidung zwischen den Operatoren, die für die

Überwachung unterschiedlicher technischer Bereiche verantwortlich sind, verringert wird. Zum Beispiel können Sie durch Korrelation von Ereignissen zu Datenbankproblemen, Netzwerkproblemen und Speicherproblemen vermeiden, dass die Operatoren aus den unterschiedlichen technischen Bereichen unabhängig voneinander unterschiedliche Ereignisse untersuchen, die Symptome ein und desselben Ursachenereignisses sind.

In Bezug auf das Auflösen komplexer Ereignisse bietet TBEC eine Reihe von Vorteilen:

- Verringert die Anzahl der angezeigten Ereignisse in der Konsole, ohne dass wichtige Daten ignoriert werden oder verloren gehen, die es Benutzern ermöglichen, durch die Hierarchie der zugehörigen Ereignisse zu navigieren und weitere Informationen zu erhalten.
- Unterstützt die domänenübergreifende Ereigniskorrelation und vereinfacht dadurch die Ursachenanalyse für Ereignisse, die Symptomereignisse generieren.
- Bei Änderungen an den topologischen Daten sind keine Änderungen an den Korrelationsregeln erforderlich.

Ereignis-Storm-Unterdrückung

Ein Ereignis-Storm liegt vor, wenn ein Problem auf einem verwalteten System auftritt, durch das in einem relativ kurzen Zeitraum eine ungewöhnlich hohe Anzahl an Ereignissen erzeugt wird. Es ist sehr wahrscheinlich, dass die Fehlerursache bereits bekannt ist und behandelt wird. Es werden aber weitere, damit in Zusammenhang stehende Ereignisse generiert. Diese Ereignisse liefern keine nützlichen Informationen, erzeugen aber eine erhöhte Last auf den Servern, auf denen die Operationenverwaltung ausgeführt wird. Um diese Situation zu vermeiden, kann die Operationenverwaltung so konfiguriert werden, dass nach Ereignis-Storms auf verwalteten Systemen gesucht wird und alle nachfolgenden Ereignisse verworfen werden, bis die Ereignis-Storm-Bedingung für ein bestimmtes System nicht mehr besteht.

Ein Ereignis-Storm wird erkannt, wenn die Anzahl an Ereignissen, die im Erkennungszeitraum aufgrund eines Problems in einem System aufgetreten sind, den für Ereignis-Storms konfigurierten Schwellenwert überschreitet.

Wenn auf einem System ein Ereignis-Storm erkannt wird, werden die Ereignisse auf diesem System verworfen, bis die Rate der eingehenden Ereignisse wieder unter den Ereignis-Storm-Schwellenwert fällt. Sie können Ausnahmeregeln konfigurieren, um Ereignisse auf einem System, auf dem zurzeit ein Ereignis-Storm besteht, mithilfe eines Filters auszuwählen und diese Ereignisse entweder im Ereignis-Browser anzuzeigen oder zu schließen (verfügbar im Ereignis-Browser unter **Geschlossene Ereignisse**). Durch das Ereignis-Storm-Endereignis wird automatisch das verknüpfte Ereignis-Storm-Anfangsereignis geschlossen.

Strukturierte Problemlösung

Die zentrale Operations Bridge optimiert den gesamten Ereignisverwaltungsprozess. Mit zentralisierten, konsolidierten Informationen können Sie konsistente, wiederverwendbare und optimierte Prozesse für die Reaktion auf Ereignisse erstellen.

Die Mehrzahl der Ereignisse in Ihrer Umgebung können Sie hochgradig strukturiert behandeln. Damit Sie Ereignisse effizienter und effektiver verwalten können, können Sie die folgenden Möglichkeiten nutzen:

- **Werkzeuge**

  Sie können Werkzeuge erstellen, um Benutzer bei der Durchführung ihrer üblichen auf CIs bezogenen Aufgaben zu unterstützen. Wenn Sie ein Werkzeug erstellen, wird es mit einem CI-Typ verbunden. Dieses Werkzeug können Sie dann in der zentralen Konsole ausführen. Zum Beispiel können Sie ein Befehlswerkzeug zum Überprüfen des Status einer Oracle-Datenbankinstanz ausführen. Das Werkzeug ist dem CI-Typ "Oracle-Datenbank" zugewiesen. Wenn Sie mehrere Versionen von Oracle-Datenbanken verwalten, müssen Sie unterschiedliche Parameter und Optionen angeben, um den Status von Oracle-Datenbankprozessen zu überprüfen. In diesem Fall können Sie mit der Funktion "Duplizieren" Kopien des am besten geeigneten Werkzeugs erstellen und an die verschiedenen Oracle-Versionen anpassen. Jedes Werkzeug ist dann für eine bestimmte Oracle-Version reserviert.

- **Benutzerdefinierte Aktionen**

  Sie können Ihre Ereignisverwaltung automatisieren, indem Sie Aktionen erstellen, die für Ereignisse ausgeführt werden, um Probleme besser lösen zu können und die Effizienz und Produktivität der Operatoren zu verbessern. Die Administratoren können viele verschiedene benutzerdefinierte Aktionen definieren, die dann beim Auflösen von Ereignissen bestimmter Typen verwendet werden. Außerdem können kontextabhängige Aktionen und kontextspezifische Werkzeuge für bestimmte Situationen definiert werden. Zum Beispiel könnten Sie einen Satz Datenbankdiagnosewerkzeuge erstellen, die speziell für die Lösung von Datenbankproblemen verwendet werden.

  Eine Anleitung zur Definition und Erstellung von Skripts, einschließlich Beispielsskripts, die mit dem Produkt bereitgestellt werden, finden Sie im *Operations Manager i Extensibility Guide*.

- **HPOM-Aktionen**

  Ereignisse aus HPOM, die im Ereignis-Browser empfangen werden, können ereignisbezogene Aktionen enthalten, die in HPOM konfiguriert wurden. Wenn ereignisbezogene Aktionen vorhanden sind, können Sie diese Aktionen über die Konsole der BSM-Operationenverwaltung ausführen. HPOM-Aktionen müssen entweder vom Operator initiiert werden oder können automatisch ausgeführt werden, wenn ein Ereignis eintritt.

  Eine vollständige Liste der verfügbaren Aktionen und Informationen dazu, wie sie ausgeführt werden, finden Sie in der Onlinehilfe zur BSM-Operationenverwaltung.

- **HP Operations Orchestration-Runbooks**

  Wenn Sie bereits HP Operations Orchestration (OO) verwenden, um Operatorenaufgaben zur Analyse und Behandlung von Problemen zu automatisieren, können diese OO-Runbooks bestimmten CI-Typen in BSM zugeordnet werden. Sie können die OO-Runbooks in einem Ereigniskontext von der Konsole der BSM-Operationenverwaltung starten.

  Zusätzlich zum manuellen Starten von Runbooks ist es auch möglich, Regeln zu konfigurieren, die die automatische Ausführung eines Runbooks oder einer Reihe von Runbooks im Kontext eines Ereignisses zur Folge haben.

  Weitere Informationen zur Ausführung von OO-Runbooks finden Sie in der Onlinehilfe zur BSM-Operationenverwaltung.

- **Diagramme**

  Grafiken und Diagramme liefern zusätzliche Daten für eine bessere Visualisierung und Analyse der leistungsbezogenen Probleme und Trends, die sich auf das CI, das durch ein Ereignis

betroffen ist, oder benachbarte CIs auswirken. Die Operatoren können auch eigene persönliche Diagramme erstellen.

Strukturierte Ereignisverwaltungsprozesse werden implementiert, um:

- Eingehende Ereignisse automatisch den Benutzern in bestimmten Benutzergruppen zuzuweisen. Durch die automatische Zuweisung von Ereignissen lässt sich die Effizienz der Ereignisverwaltung erhöhen und die Zeitverzögerung bis zu einer möglichen Reaktion auf das Ereignis verkürzen. Der Systemadministrator im Bereich IT-Betrieb kann die BSM-Operationenverwaltung so konfigurieren, dass eingehende Ereignisse automatisch verfügbaren Operatorgruppen zugewiesen werden, die für das Auflösen dieser Ereignisse verantwortlich sind.
- Nach einer angegebenen Zeit Aktionen für Ereignisse zu starten, die bestimmte Kriterien erfüllen. Die Regeln für die zeitbasierte Ereignisautomatisierung bestehen aus drei Hauptelementen:
  - Filter, mit denen Ereignisse definiert werden, auf die die Regeln für die zeitbasierte Ereignisautomatisierung angewendet werden sollen.
  - Zeitraum zur Definition der Dauer, für die ein Ereignis mit dem Filter der Regel übereinstimmen muss, damit die Aktionen der Regel für dieses Ereignis gestartet werden.
  - Liste der Aktionen, die bei übereinstimmenden Ereignissen gestartet werden sollen. Folgende Aktionen sind verfügbar: erneutes Ausführen automatischer Aktionen für Ereignisse, Ändern von Ereignisattributen, Weiterleiten von Ereignissen an externe Server, Zuweisen von Ereignissen zu Benutzern und Gruppen, Ausführen von Skripts und Ausführen von Runbooks.
- Den Status von Ereignissen unter Verwendung von Konzepten zur Lebenszyklusverwaltung anzuzeigen und zu überwachen. Neben allen Benutzern, die in der Lösung bereits eine Rolle gespielt haben, können Sie auch erkennen, wer gerade an der Auflösung des Ereignisses arbeitet.
- Zu dokumentieren, wie ein Ereignis behandelt und gelöst wird. Sie können das Ereignis mit Anmerkungen zur Beschreibung des Problemlösungsprozesses versehen oder Fachwissen bereitstellen, indem Sie Ereignisse mit Tipps und Hinweisen versehen, die das Verständnis verbessern und das dem Ereignis zugrunde liegende Problem erläutern.

Verwalten von Inhalten mit Content Packs

Inhalt besteht aus Informationen, die von BSM verwendet werden, um die Objekte oder Konfigurationselemente (Configuration Items, CIs) zu beschreiben und zu erweitern, die die in der IT-Umgebung überwachten Elemente darstellen. Bei diesen Objekten kann es sich z. B. um Netzwerkhardware, Betriebssysteme, Applikationen, Services oder Benutzer handeln. Der Inhalt dient dazu, die Daten von Konfigurationselementen zu erweitern.

Die Configuration Item-Daten, die speziell für die BSM-Operationenverwaltung gedacht sind, werden Content Packs verwaltet. Den Inhalt können Sie als Satz vieler Content Packs betrachten. Content Packs enthalten vorkonfigurierte Regeln, Werkzeuge (auch Runbooks) und weitere Elemente für bestimmte verwaltete Applikationen und Systeme. Damit kann ein Content Pack eine Momentaufnahme Ihres gesamten Inhalts oder eines Teils davon enthalten. Content Packs dienen auch dem Austausch angepasster Daten zwischen Instanzen von BSM, z. B. in Test- und Produktionsumgebungen. Sie können Inhalte auch für mehrere Content Packs nutzen.

Content Packs enthalten in der Regel die folgenden Elemente:

- Korrelationsregeln
- Zuordnungsregeln für die Topologiesynchronisierung
- Definitionen von Zustandsindikatoren (Health Indicators, HIs) mit Zuordnungsregeln
- Definitionen von Ereignistypindikatoren (ETIs) mit Zuordnungsregeln
- Regeln und Zuweisungen für zentrale Leistungsindikatoren (Key Performance Indicators, KPIs)
- Menüs
- Ansichtszuordnungen
- Diagramme und Diagrammzuordnungen
- Werkzeuge
- Definitionen für EPI-Skripts (Event Processing Interface, Ereignisverarbeitungsschnittstelle) und für Skripts für benutzerdefinierte Aktionen
- Ereignisweiterleitungsregeln

Inhalte, die nicht speziell für die BSM-Operationenverwaltung gedacht sind (wie zum Beispiel zusätzliche CI-Typen), befinden sich in anderen Packs, die mit speziellen Werkzeugen gesondert verwaltet werden.

Es gibt zwei Arten von Content Packs:

- Standardmäßig verfügbare Content Packs zur Ergänzung der Daten, die zum Beispiel durch NNMi oder HP Operations Manager-Smart Plug-Ins (SPIs) gesammelt werden.
- Benutzerdefinierte Content Packs, die Sie selbst entwickeln, um die Anforderungen Ihrer eigenen Applikationen und Überwachungsrichtlinien zu erfüllen.

Die benutzerdefinierten Content Packs werden in der Regel vom Entwickler von Überwachungslösungen erstellt und dann vom Systemadministrator im Bereich IT-Betrieb implementiert.

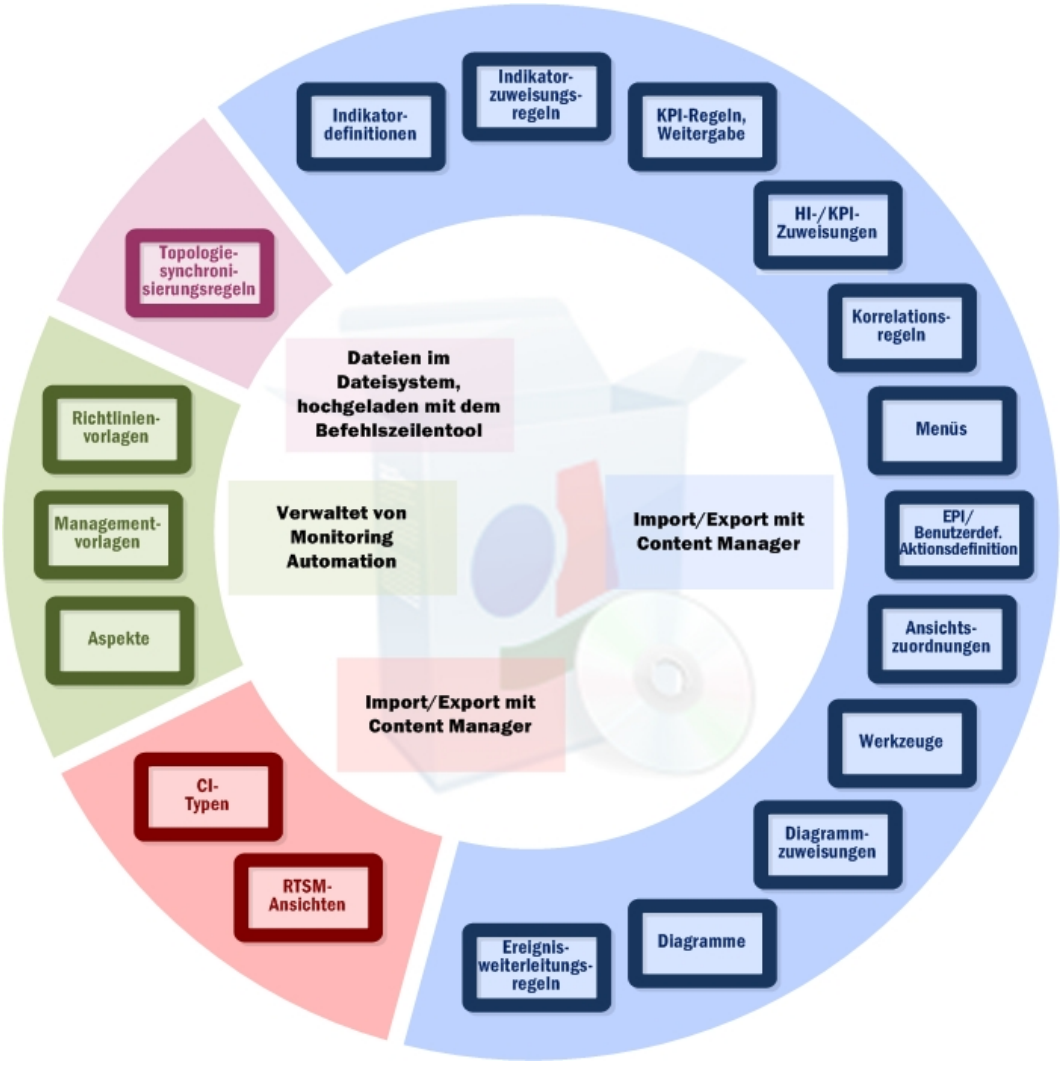
Vordefinierte Content Packs

Wenn der Systemadministrator die HP Operations Manager-Content Packs implementiert, stellt er die notwendigen Konfigurationsdaten für den Empfang und die Verarbeitung der aus HP Operations Manager weitergeleiteten Ereignisse bereit.

Wenn der Systemadministrator zum Beispiel das Content Pack für die Oracle-Datenbank installiert, stellt er für die BSM-Operationenverwaltung die Informationen über Form und Inhalt der Ereignisse bereit, die durch das HP Operations Manager-Smart Plug-In für Oracle-Datenbanken gesendet werden. Das Content Pack enthält die Definitionen der Regeln, Werkzeuge und Diagramme, die benötigt werden, um Ereignisdaten für die Ermittlung des Zustands von Oracle-CIs oder die Korrelation von Oracle-Ereignissen zu verwenden. Und das Infrastruktur-Content Pack als ein anderes Beispiel stellt die notwendigen Konfigurationsdaten (auch Werkzeuge) für die Integration von Ereignissen aus NNMi bereit.

Abbildung 4 auf der nächsten Seite enthält eine Übersicht über den Inhalt, der sich in einem Satz Content Packs befinden kann.

Abbildung 4 – Inhalt, der sich in einem Satz von Content Packs befinden kann



Werkzeuge zur Verwaltung von Inhalten

BSM enthält Werkzeuge zur Verwaltung von Inhalten. Mit Content Manager können Sie Inhalte auch zwischen Systemen austauschen. Zum Beispiel können Sie den Inhalt in einer Testumgebung vorbereiten und, wenn der Test bestätigt, dass dieser Inhalt wie erwartet funktioniert, den getesteten Inhalt dann an eine Produktionsumgebung übertragen.

Mit den Werkzeugen für den Export und den Import können Sie Inhalte zwischen Systemen austauschen, damit Sie über Momentaufnahmen oder Backup-Images des entwickelten Inhalts verfügen und zusätzlich sicherstellen können, dass die unterschiedlichen Instanzen immer synchronisiert und aktuell sind.

Skalierbare Architektur mit mehreren Servern

Die BSM-Operationenverwaltung ermöglicht Ihnen die Verwaltung weit verteilter Systeme von einer zentralen Stelle aus. In einer verteilten Implementierung können Sie Ihre Umgebung hierarchisch konfigurieren. Danach können Sie die Verantwortlichkeit für das Management über mehrere

Managementebenen verteilen, wobei Sie bestimmte Kriterien wie Fachkompetenz der Operatoren, geografischer Standort und Tageszeit zugrunde legen. Durch dieses flexible Management können sich die Operatoren auf ihre Spezialaufgaben konzentrieren und von einer technischen Unterstützung profitieren, die rund um die Uhr automatisch und auf Abruf verfügbar ist.

Dank der skalierbaren Architektur können eine oder mehrere Instanzen der BSM-Operationenverwaltung zu einer einzelnen leistungsstarken Managementlösung kombiniert werden, sodass die Anforderungen Ihrer Organisationsstruktur erfüllt werden. Dadurch können Sie Server so konfigurieren, dass sie Ereignisse an andere Server in Ihrer Umgebung weiterleiten.

In einer verteilten Umgebung können Server, auf denen die BSM-Operationenverwaltung gehostet wird, so konfiguriert werden, dass sie nicht nur mit anderen ähnlichen Servern, sondern auch mit mehreren HPOM for Windows- und HPOM for UNIX-Management-Servern, anderen BSM-Servern und sogar Domänen-Managern von Drittanbietern zusammenarbeiten.

In einer solchen hierarchischen, verteilten Umgebung können Sie die BSM-Operationenverwaltung für die folgenden Zwecke konfigurieren:

- Für die Funktion als "Manager of Managers" (MoM), also für die zentrale Ereigniskonsolidierung der gesamten Umgebung an der Spitze der Hierarchie.
- Für die Zusammenarbeit mit anderen HP-Produkten, wie zum Beispiel NNMi und HP SiteScope.
- Für die Zusammenarbeit mit Domänen-Managern von Drittanbietern, wie zum Beispiel Microsoft Systems Center Operations Manager.

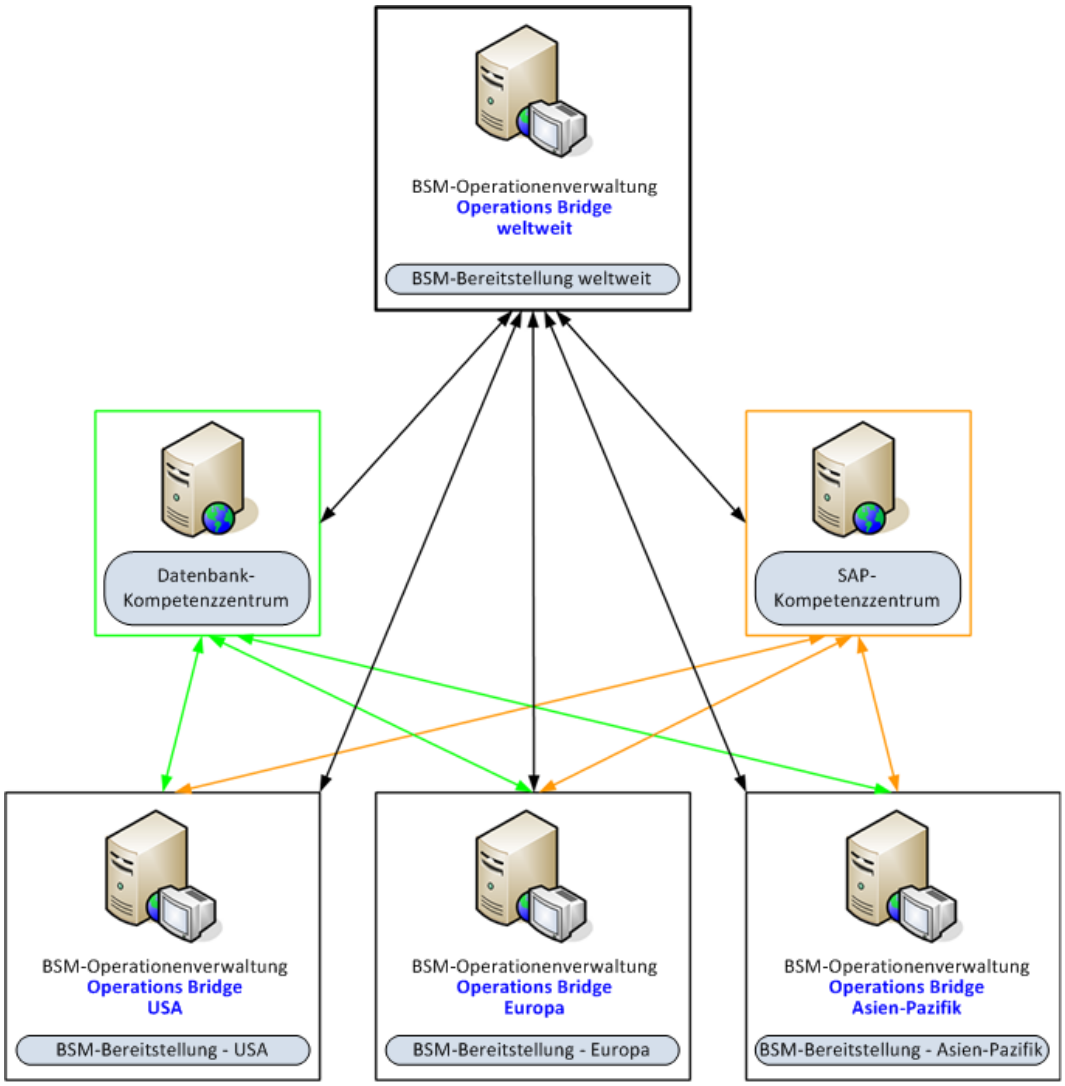
Sie können Server, auf denen die BSM-Operationenverwaltung gehostet wird, für folgende Zwecke konfigurieren:

- Für die Weiterleitung von Ereignissen an andere Server, auf denen die BSM-Operationenverwaltung gehostet wird, und für die serverübergreifende Synchronisierung dieser Ereignisse.
- Für den Empfang von Nachrichten, die von mehreren HPOM for Windows- und HPOM for UNIX-Management-Servern weitergeleitet werden, und für die Synchronisierung dieser Nachrichten zwischen Servern, auf denen die BSM-Operationenverwaltung gehostet wird, und HPOM-Management-Servern.
- Für den Empfang von Ereignissen, die von einem BSM-Server weitergeleitet werden, der von BSM-Komponenten, wie zum Beispiel HP Business Process Monitor (BPM), Warnungen empfängt.

Manager-of-Managers

Abbildung 5 auf der nächsten Seite zeigt ein Beispiel für eine hierarchische, verteilte Umgebung mit einem zentralen Server, auf dem die BSM-Operationenverwaltung gehostet wird und der nach dem Prinzip des serverbasierten flexiblen Managements andere regionale Server, auf denen die BSM-Operationenverwaltung gehostet wird, verwaltet.

Abbildung 5 – Manager-of-Managers-Implementierung (MoM)



In diesem Beispiel verwalten die Implementierungen auf den regionalen Servern "BSM Europe", "BSM USA" und "BSM Asia Pacific" unterschiedliche Regionen. Die BSM-Operationenverwaltung, die auf der Serverimplementierung "BSM Worldwide" gehostet wird, befindet sich an der Spitze der Hierarchie und verwaltet die regionalen Server. Dies ist der MoM, also die zentrale Ereigniskonsole für die gesamte Umgebung. Es handelt sich um eine weltweite Operations Bridge. Die regionalen Server können in ihren Regionen auch als MoM für untergeordnete Systeme agieren, damit eine regional überwachte Umgebung entsteht. Das Management überwachter Umgebungen in einer hierarchischen Struktur kann kaskadenförmig gestaltet werden.

Wenn Sie in einem großen Unternehmen mit mehreren weit verteilten Management-Servern arbeiten, ist Fachwissen zu einem bestimmten Thema nicht immer lokal verfügbar. Zum Beispiel könnte Ihre Organisation ein spezielles Kompetenzzentrum für SAP besitzen. Zusätzlich könnte es ein weiteres spezielles Kompetenzzentrum für Datenbanken geben.

In einer Hierarchie mit Kompetenzzentren wird die Verantwortlichkeit für Konfigurationselemente in der überwachten Umgebung verteilt. Regionale Server sind nicht allein für Konfigurationselemente verantwortlich.

Stattdessen werden Ereignisse zu bestimmten Themen an einen Kompetenzzentrumsserver weitergeleitet, auf dem das Fachwissen vorhanden ist, um ähnliche Probleme für alle Konfigurationselemente in der überwachten Umgebung zu lösen.

In einer verteilten Umgebung kann der Systemadministrator im Bereich IT-Betrieb regionale Server so konfigurieren, dass bestimmte Nachrichten an andere Server im Netzwerk weitergeleitet werden. Derselbe Systemadministrator regionale Server so konfigurieren, dass Ereignisse auf der Basis von Ereignisattributen an einen beliebigen Server im Netzwerk weitergeleitet werden.

In Abbildung 5 auf der vorherigen Seite leiten alle regionalen Server (BSM Europe, BSM USA und BSM Asia Pacific) alle datenbankbezogenen Ereignisse an den Server mit dem Datenbank-Kompetenzzentrum und alle SAP-bezogenen Ereignisse an den Server mit dem SAP-Kompetenzzentrum weiter.

In einem solchen Szenario synchronisiert die Operations Bridge die Ereignisaktionen (zum Beispiel Auflösen, Zuweisen, Ändern des Schweregrads) zwischen den regionalen Servern und den Kompetenzzentren. Dies stellt sicher, dass die Ereignisse hinsichtlich ihres Status in der gesamten Unternehmensumgebung immer synchronisiert sind.

Monitoring Automation

Überwachung (Monitoring) ist die Generierung von Ereignissen, wenn ein CI ein unerwartetes Verhalten aufweist. Typische Ereignisse sind:

- Ein überwachter Wert überschreitet einen bestimmten Schwellenwert. Beispiel: Der für eine Datenbank verwendete Speicherplatz überschreitet einen vordefinierten Grenzwert von 90 %.
- Ein Knoten wurde aus dem Netzwerk entfernt. Beispiel: Ein Stromausfall führt zum Herunterfahren eines Servers, sodass dieser nicht mehr erreicht werden kann.

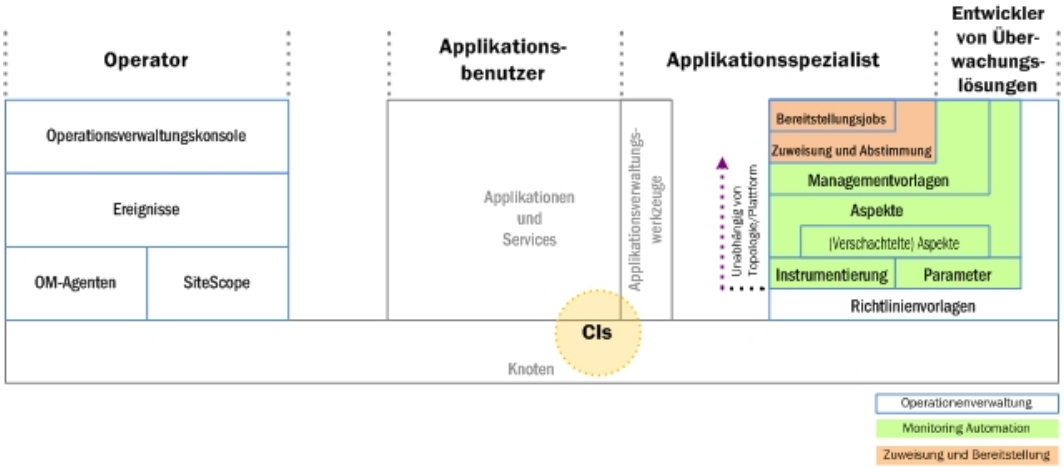
Monitoring Automation bietet eine umfassende Verwaltungslösung für eine Applikation oder einen Service, wodurch es Ihnen möglich ist, eine Verwaltungslösung für den gesamten Satz an CIs (Configuration Items, Konfigurationselemente) zu erstellen, aus denen sich die Applikation zusammensetzt. Die Lösung kann so konfiguriert werden, dass sie dynamisch auf Änderungen in der Topologie reagiert, wodurch die Überwachungslösung unabhängig von der Hardware und Plattform ist, auf der die Applikation ausgeführt wird.

Der Schlüssel zum Verständnis von Monitoring Automation ist das Verständnis der zugrunde liegende Terminologie und Architektur. Sehen Sie sich den in Abbildung 6 auf der nächsten Seite dargestellten Stapel an. Die Basis des Stapels steht für die CIs, die überwacht werden sollen. CIs können Netzwerkelemente wie Computer aber auch Applikationen oder Gruppen von Applikationen sein, die einen Service bereitstellen. Der Zugriff auf CIs erfolgt auf folgende Weise:

- Benutzer interagiert mit den CIs unabhängig von jeder Überwachung, wie im zentrale Abschnitt von Abbildung 6 auf der nächsten Seite angedeutet wird.
- Die Operationenverwaltung überwacht die CIs mithilfe der vertrauten Überwachungsstruktur, wie im linken Abschnitt von Abbildung 6 auf der nächsten Seite gezeigt wird.
- Ein Entwickler konfiguriert Überwachungslösungen, wie im rechten Abschnitt von Abbildung 6 auf der nächsten Seite gezeigt wird.
- Nachdem die vom Entwickler erstellte Konfiguration optimiert wurde, startet ein Applikationsspezialist den Überwachungsprozess und reagiert auf die vom Operator

übergebenen Ereignisse, indem Bereitstellungsjobs untersucht und applikationsspezifische Verwaltungswerkzeuge verwendet werden.

Abbildung 6 – Operationenverwaltungsstapel



Monitoring Automation bietet eine Reihe von Funktionen für die Erstellung von flexiblen Überwachungslösungen. Im folgenden Abschnitt werden die einzelnen Begriffe oder Funktionen erläutert, die in Abbildung 6 oben dargestellt sind. Nach dem Lesen sollten Sie die zugrunde liegenden Prinzipien verstehen. Die Erklärung erfolgt in der Reihenfolge der Ebenen des Konfigurationsstapels von unten nach oben.

Knoten

Ein Knoten ist ein physisches Element, auf das Sie im Netzwerk zugreifen können.

CI

Ein CI ist ein Knoten oder eine Applikation oder ein Service, die bzw. der auf einem Knoten ausgeführt wird. CIs sind der eigentliche Gegenstand der Überwachung durch die Operationenverwaltung. Ereignisse beziehen sich immer auf CIs.

Richtlinienvorlagen

Richtlinienvorlagen legen fest, was überwacht wird und wie die Überwachung durchgeführt wird. Beachten Sie, dass die Richtlinienvorlagen plattformabhängig sind.

Vor dem Einsatz von Monitoring Automation wurden alle Konfigurationen über Richtlinien und Richtlinienvorlagen vorgenommen. Dies bedeutet, dass für jede Änderung in einem CI (in Hinblick auf die Plattform, die Topologie oder die Überwachungsrichtlinie) die Werte in den CI-Richtlinienvorlagen, auf deren Grundlage das CI überwacht wird, geändert werden mussten.

Parameter und Instrumentierung

Mit Monitoring Automation wird die Verwendung von Parametern eingeführt. Jeder Parameter entspricht einer Überwachungseinstellung für ein einzelnes CI-Attribut in der Richtlinienvorlage. Durch das Ändern der Parameterwerte ändert sich das Überwachungsverhalten, da die hartcodierten Werte in einer Richtlinienvorlage nicht mehr geändert werden müssen. Das Konzept der kaskadenförmigen Anordnung von Standardwerten ist von zentraler Bedeutung für Monitoring Automation. Die Idee ist, dass der Entwickler oder Applikationsspezialist so viele Standardwerte

wie möglich auf einer bestimmten Ebene verwendet und so einen Basiswert für die Überwachung erstellt. Auf der nächsten oberen Ebene kann und muss eine Teilmenge dieser Werte für die jeweilige Überwachungsaufgabe überschrieben werden, wobei jeder Wert, der bereits von der Basiswerteinstellung abgedeckt ist, übernommen werden kann, ohne dass er neu definiert werden muss.

Die folgenden Parameterfeatures bieten zusätzliche Flexibilität:

- Bedingte Parameterwerte ermöglichen die Verwendung des gleichen Parameters mit mehreren Richtlinienvorlagen, wodurch hardware- und plattformunabhängige Überwachungslösungen möglich werden.
- Parameter mit dem gleichen Wert können in einem einzigen Parameter kombiniert werden. Hierdurch ist es nicht mehr notwendig, den gleichen Wert mehrmals einzugeben.

Die Instrumentierung umfasst von HP Operations Agent ausgeführte Skripts und Programme gemäß Definition in den Richtlinien für verwaltete Knoten, auf denen der Agent installiert ist.

Aspekte

Richtlinienvorlagen und Instrumentierung, die ein bestimmtes erwartetes Verhalten der Applikation oder des Service darstellen, die oder der überwacht werden soll, werden in Aspekten gruppiert. Auf Aspektebene wird die Konfiguration von Entwicklern folgendermaßen optimiert:

- Sie kombinieren Parameter mit derselben Funktion in einzelnen Parametern.
- Sie können Aspekte verschachteln, um Aspekte, die das gleiche Verhalten darstellen, jedoch in verschiedenen Richtlinienvorlagen definiert sind, in einem einzigen Aspekt zu kombinieren. Jeder verschachtelter Aspekt kann mit einer Bereitstellungsbedingung gepaart werden, die an die Operationenverwaltung weitergibt, welcher verschachtelter Aspekt in welcher Umgebung verwendet werden muss. Dies ermöglicht es jedem CI des Ziel-CI-Typs, den gleichen Aspekt unabhängig von der Plattform zu verwenden.
- Sie legen Standardwerte auf Aspektebene fest, die im Einklang mit den Überwachungsrichtlinien des Unternehmens stehen.

Managementvorlage

In einer Managementvorlage werden alle Aspekte kombiniert, die für die Überwachung von zusammengesetzten Applikationen oder Services notwendig sind. Die Managementvorlagenkonfiguration umfasst die Topologie der zusammengesetzten Applikation und die zu überwachenden Aspekte. Darüber hinaus setzt der Entwickler alle unternehmensweiten Standardwerte auf Ebene der Managementvorlage außer Kraft, falls dies für die zu überwachende Applikation erforderlich ist.

Der Entwickler übergibt die fertige Managementvorlage an den Applikationsspezialisten, der sie verwendet, um mit der Überwachung der Zielapplikation zu beginnen.

Optimierung, Zuweisung und Bereitstellung

Vor dem Start des Überwachungsprozesses kann der Applikationsspezialist, falls gewünscht, bestimmte vom Entwickler konfigurierte Standardwerte außer Kraft setzen, um situationsspezifischen Überwachungsanforderungen Rechnung zu tragen. Dies wird Optimierung genannt.

Die Überwachungskonfiguration, die durch einen Aspekt dargestellt wird, wird in Bezug auf einen CI-Typ definiert. Damit die Operationenverwaltung mit der Überwachung beginnen kann, muss

dieser CI-Typ einer tatsächlichen CI-Instanz zugeordnet werden, die im Rahmen der Topologie-Discovery ermittelt wurde. Diese Zuordnung wird Zuweisung genannt und kann auf folgende Weise erfolgen:

- Manuelle Zuweisung einer Managementvorlage. Der Applikationsspezialist verknüpft die Managementvorlage mit einer CI-Instanz des Stamm-CI der Managementvorlage.
- Manuelle Zuweisung eines Aspekts. Der Applikationsspezialist verknüpft den Aspekt mit einer CI-Instanz des Ziel-CI-Typs des Aspekts.
- Automatische Zuweisung. Wenn der Applikationsspezialist automatische Zuweisungen für eine Managementvorlage oder einen Aspekt definiert, weist die Operationenverwaltung dynamisch Aspekte zu den relevanten CI-Instanzen zu, sobald diese ermittelt werden.

Nachdem die Zuweisung abgeschlossen ist, wird die Überwachungslösung im gleichen Schritt bereitgestellt. Während die Überwachung ausgeführt wird, kann der Applikationsspezialist alle Bereitstellungsjobs im Blick behalten, um sicherzustellen, dass der Überwachungsprozess wie erwartet verläuft, oder um Informationen zu erfassen, die mit Ereignissen in Zusammenhang stehen, die von einem Operator gemeldet wurden.

Benutzerbindung

Das innovative Feature "Benutzerbindung" setzt Spielmechanismen ein, um die Benutzer der Operationenverwaltung zusätzlich zu animieren, indem geschäftsfördernde Herausforderungen bereitgestellt werden, die die Effizienz der Operations Bridge und das Know-how der Benutzer fördern. Das erfolgreiche Absolvieren der verschiedenen Stufen wird mit Auszeichnungen und Echtzeit-Benachrichtigungen über die herausragende Leistung belohnt, um die intensivere Beschäftigung mit der Operationenverwaltung weiter zu fördern und auf diese Weise die Leistung der Benutzer bei ihrer täglichen Arbeit zu verbessern. Anhand von Zeitachsen kann der Fortschritt jedes Benutzers und das Erzielen von Auszeichnungen aufgezeichnet werden. Fast jeder Benutzer lässt sich durch mindestens eine der Herausforderungsarten motivieren, die durch Spielmechanismen verfügbar sind, beispielsweise Auszeichnungen, Wettbewerb, Status und Lösung einer Aufgabe, was "Benutzerbindung" zu einem leistungsfähigen Feature macht.

Durch das Festlegen geschäftsorientierter Auszeichnungen, auf die die Benutzer der Operationenverwaltung hinarbeiten, und die Vergabe von Belohnungen, wenn die gewünschten Aufgaben erledigt wurden, werden die wichtigsten Kompetenzen erworben und die wichtigsten Aufgaben erledigt, während gleichzeitig das Engagement und die Spannung bei der Ausführung der täglichen Aufgaben gefördert wird. Benutzer können zusehen, wie sich durch ihre Arbeit ihre Fortschrittsleisten füllen, und ihren Fortschritt über ihre Aufgaben und Herausforderungen in ihren Dashboards abbilden. Mit dem Erreichen jeder neuen Auszeichnung kann eine Popup-Benachrichtigung einhergehen, die eine sofortige Rückmeldung über gute Leistung bereitstellt.

"Benutzerbindung" nutzt intrinsische Beweggründe, um die Benutzer der Operationenverwaltung anzuspornen, die gesetzten Ziele zu erreichen. Externe Belohnungen, die in der Regel nur von vorübergehendem Nutzen, sind nicht notwendig. Menschen möchten erfolgreich sein und wünschen sich, dass ihr Erfolg auch wahrgenommen wird. "Benutzerbindung" bietet ein Gerüst, mit dem Sie den Benutzern helfen können, die Verwendung der Operationenverwaltung zu erlernen und ihren täglichen Aufgaben besser gerecht zu werden, da es Leistungen sichtbar macht und somit die Freude und das Engagement bei der Arbeit erhöht.

Administratoren des Features "Benutzerbindung" können integrierte Auszeichnungen auswählen, konfigurieren und aktivieren, die an die Bedürfnisse der verschiedenen Benutzer der

Operationenverwaltung angepasst sind. Benutzer können die erste Leistungsebene absolvieren und werden nach dem erfolgreichen Erreichen von Auszeichnungen eingeladen, die nächste Stufe in Angriff zu nehmen, sodass sie sich ihrer Leistung und ihrer Fortschritte besser bewusst werden.

Integrationsschnittstellen

Die bereitgestellten Schnittstellen ermöglichen die Integration mit anderen Applikationen und die Modifikation und Anpassung des Ereignisverwaltungsprozesses. Beispiel:

- Um Ereignisse während der Ereignisverarbeitung zu modifizieren und zu erweitern, können mit einer Ereignisverarbeitungsschnittstelle einzelne Ereignisverarbeitungsskripts in die Ereignisverarbeitungspipeline integriert werden. Dies ermöglicht Ihnen die Erweiterung (Anreicherung) von Ereignissen:
  - Während der Ereignisverarbeitung, zum Beispiel durch Hinzufügen von Informationen, die bei der CI-Auflösung und ETI-Auflösung verwendet werden, oder durch Beeinflussung der Art der Behandlung doppelter Ereignisse.
  - Zur Bereitstellung weiterer Informationen nach der Ereignisverarbeitung, zum Beispiel zusätzliche Informationen zu CIs aus Ressourcendatenbanken oder nützliche Informationen für die Fehlerbehebung, wie zum Beispiel einen Drilldown-URL oder einen Link zu einer externen Wissensdatenbank.
- Zur Integration von Ereignissen in andere Applikationen ermöglicht eine Ereignisschnittstelle als Webservice den Entwicklern und Integrationsverantwortlichen die Automatisierung von Operatorfunktionen und die Erkennung von Änderungen an Ereignissen. Die meisten Dinge, die ein Operator in der Konsole tun kann, während er an Ereignissen arbeitet, können auch programmgestützt erledigt werden, was die Effizienz deutlich erhöhen würde. Diese Schnittstelle stellt auch eine Unterstützung für Abonnements über die Atom-Feed-Funktionalität bereit.
- Zur Synchronisierung von Ereignissen zwischen der BSM-Operationenverwaltung und einer externen Ereignisverarbeitungsapplikation stellt die BSM-Operationenverwaltung eine Webserviceschnittstelle für die Ereignissynchronisierung bereit. Ein typischer Anwendungsfall ist die Synchronisierung von Ereignissen zwischen der BSM-Operationenverwaltung und einem Vorfall-Manager, wie zum Beispiel Service Manager.
- Zur direkten Integration mit anderen Domänen-Managern, wie zum Beispiel Microsoft Systems Center Operations Manager, stellt BSM den HP BSM Integration Adapter bereit.

Im *Operations Manager i Extensibility Guide* in der HP Business Service Management-Dokumentationsbibliothek finden Sie die Beschreibung dieser Schnittstellen sowie Informationen für Entwickler von Inhalten und Integrationsverantwortliche, wie die Funktionalität der BSM-Operationenverwaltung angepasst und erweitert werden kann.

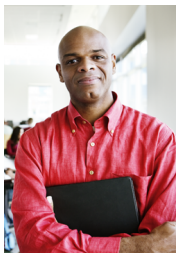
Benutzerrollen und Verantwortlichkeiten

Für das Installieren, Konfigurieren und Ausführen der Operations Bridge ist ein Team aus Personen mit speziellen Fähigkeiten und Fachkenntnissen erforderlich. Jede Rolle zeichnet sich durch eigene Verantwortlichkeiten und Aufgaben aus.

- Der Operator ist der praktische Ereignismanager und Problemlöser.
- Der Entwickler von Überwachungslösungen kennt sowohl das Überwachungsprodukt als auch die Applikation gut genug, um die Überwachungslösung zu entwickeln. Er entscheidet über die zu überwachenden Elemente und die entsprechenden Leistungsebenen.
- Der Systemadministrator im Bereich IT-Betrieb installiert und konfiguriert die Überwachungs- und Ereignisverwaltungsprozesse. Was er konfigurieren kann, ist sehr flexibel. Er fügt in der BSM-Benutzerverwaltung neue Benutzer entsprechend den lokalen Anforderungen hinzu. Er kann Berechtigungen erteilen und den Zugriff auf Verwaltungsbenutzeroberflächen, Werkzeugkategorien und benutzerdefinierte Aktionen einschränken. Er kann Rechte und Berechtigungen für einzelne Benutzer oder Benutzertypen festlegen. Er kann auch den Zugriff auf Ereignisse, die anderen Benutzern zugewiesen sind, ermöglichen oder sperren. Zum Beispiel kann er Benutzern ermöglichen, Ereignisse, die ihnen nicht zugewiesen sind, anzuzeigen, aber ihnen das Recht, Änderungen vorzunehmen, verweigern.
- Der Applikationsspezialist weiß alles über eine bestimmte Applikation oder einen bestimmten Service. Er verwaltet die Ausstattung, die an der Ausführung der Applikation beteiligt ist, und behebt Probleme, falls Überwachsereignisse auf ein Problem hinweisen.

In Tabelle 1 auf der nächsten Seite finden Sie häufig verwendete Titel für diese Benutzerrollen sowie eine Übersicht über ihre Verantwortlichkeiten. Nachdem wir nun mehr über die BSM-Operationenverwaltung wissen, werden wir in den folgenden Kapiteln einige typische Benutzer begleiten, um zu sehen, wie sie ihren Arbeitstag organisieren und ihre Aufgaben erfüllen. In nächsten Kapitel erfahren wir mehr über die täglichen Verantwortlichkeiten des Operators Dave in einer Unternehmensumgebung, in der die BSM-Operationenverwaltung als Operations Bridge fungiert.

Tabelle 1 – Benutzerrollen

Stellenbezeichnung	Weitere Bezeichnungen	Verantwortlichkeiten
Operator  "Dave"	• Domänenoperator • Operator im Bereich IT-Betrieb	Überwacht täglich die Ereignisse, die ihm oder seiner Arbeitsgruppe zugewiesen wurden. Führt außerhalb der BSM-Operationenverwaltung Routineoperationen für die Applikationen, Systeme und Netzwerke aus, für die er verantwortlich ist. Behebt Probleme mit Ereignissen, die zu einem Vorfall eskalieren könnten.
Entwickler von Überwachungslösungen  "Mike"	• Fachmann • Entwickler von Überwachungslösungen im Bereich IT-Betrieb • Fachexperte für Applikationen, Netzwerke oder Spezialgebiete	• Passt die Art und Weise an, wie die BSM-Operationenverwaltung eine Domäne überwacht. • Konfiguriert Managementvorlagen, Aspekte und Richtlinienvorlagen für Monitoring Automation.
Administrator  "Matthew"	• Systemadministrator • Systemadministrator im Bereich IT-Betrieb • Administrator der BSM-Operationenverwaltung • Systemarchitekt	Überwacht die BSM-Operationenverwaltungsumgebung und Aufgabenzuweisungen. Verknüpft die BSM-Operationenverwaltung mit anderen Werkzeugen und Prozessen.
Applikationsspezialistin  "Alice"	• Expertin für eine bestimmte Applikation oder einen bestimmten Service • Applikationsadministrator	Optimiert eine Überwachungslösung für die jeweilige Applikations- oder Serviceumgebung und weist Managementvorlagen oder Aspekte zu Systemknoten zu. Implementiert die Überwachungslösung und stellt sicher, dass die Überwachung ordnungsgemäß ausgeführt wird.

Workflow des Operators

Im Kapitel "Einführung in die BSM-Operationenverwaltung" haben wir Dave kennengelernt. Dave ist der Operator, der für das tägliche Management einer BSM-Bereitstellung verantwortlich ist. Ein Operator ist in der IT-Umgebung eines Unternehmens in der Regel eine Einstiegsposition, aber Dave verfügt über diverse Fähigkeiten, da er bereits Erfahrungen mit vielen Technologien gesammelt hat, die in der BSM-Operationenverwaltungsumgebung zum Einsatz kommen.

Dave arbeitet zu den verschiedensten Zeiten, da er oft gerufen wird, wenn Probleme auftreten. Um sicherzustellen, dass seine Benutzer ohne Unterbrechung arbeiten können, kann er das Problem dann entweder vor Ort lösen oder sich über Fernzugriff anmelden. Die Benutzeroberfläche der BSM-Operationenverwaltung ermöglicht ihm die Überwachung der Ereignisse in seinem Bereich von jedem beliebigen Standort aus, solange er Zugriff auf das Netzwerk hat.

Dave muss die Ereignisverwaltung genau kennen und wissen, wie er die zustandsbezogenen Werkzeuge nutzen muss, die ihm zur Verfügung stehen. Es gibt Werkzeuge, selbst-konfigurierende Befehle, Skripts und Links zu weiteren Informationen, die Operatoren wie Dave helfen, Ereignisse verschiedener Typen, die in der Betriebsumgebung auftreten, aufzulösen und zu schließen.

Die Operations Bridge ermöglicht es Dave, Warnungen und Ereignisse in seinem Bereich sofort zu sehen. Er kann sich auf die automatische Verwaltung dieser Ereignisse und Behebung der zugrunde liegenden Probleme mit den geeigneten Werkzeugen konzentrieren.

Dave bringt seinem Unternehmen einen Nutzen, da er die Ereignisse in seinem Bereich nach ihren Auswirkungen auf Geschäftsservices und Kontinuität priorisiert. Kleine Probleme muss Dave beheben, bevor sie zu großen Problemen werden, die zu einer Verschlechterung der Qualität der unterstützten Geschäftsservices führen.

Seine Erfahrung mit den zugrunde liegenden Technologien kann Dave helfen, Ereignisse zu korrelieren, die in verschiedenen technischen Bereichen auftreten, wie zum Beispiel: Datenbanken, Hardware, Netzwerk, Webapplikationen usw. Er überwacht diese unterschiedlichen Technologien, um die Auswirkungen eines Fehlers in einem Bereich, der die Reaktionsfähigkeit des Systems in einem anderen Bereich beeinträchtigen könnte, zu minimieren. Indem Probleme minimiert werden, bevor sie eskalieren, wird die Unternehmensproduktivität verbessert, da der Kaskadeneffekt bei einem nicht erkannten kritischen Ereignis minimiert wird.

Wenn Dave ein Problem nicht beheben kann, kann er es eskalieren, indem er das Ereignis an eine externe Ereignisverarbeitungsapplikation weiterleitet. Dies umfasst in der Regel auch die

Übertragung des Ereignisbesitzes, beispielsweise an einen Helpdesk-Operator oder einen Applikationsspezialisten.

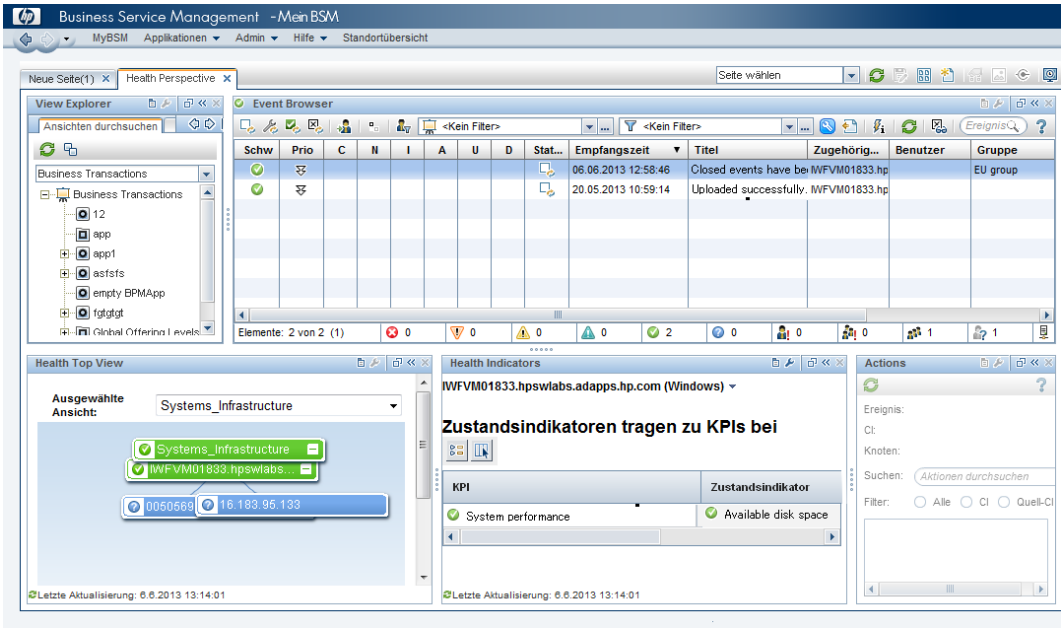
Die Umgebung des Operators

Der Systemadministrator definiert Benutzerrollen und weist Benutzerrechte zu und legt damit fest, welche Ereignisse jeder Operator anzeigen oder modifizieren kann. Dave kann die ihm zugewiesenen Ereignisse sowie weitere Ereignisse, für die es ihm gestattet ist, in einer domänenübergreifenden Ansicht anzeigen. Zum Beispiel ist er für die Wartung des E-Mail-Servers des Unternehmens verantwortlich, könnte aber auch Ereignisse sehen, die einem anderen Operator zugewiesen wurden.

Zustandsperspektive

Abbildung 7 unten zeigt die Registerkarte "Zustandsperspektive" mit fünf Bereichen, in denen unterschiedliche Ansichten des Systems angezeigt werden. Dave beginnt jeden Arbeitstag mit dem Öffnen der Zustandsperspektive.

Abbildung 7 – Zustandsperspektive



Die fünf Bereiche bieten eine globale Ansicht der Ereignisse in Daves Zuständigkeitsbereich:

- Im Modell-Explorer kann Dave eine Ansicht und einen Bereich, für den er verantwortlich ist, auswählen. In der Ansicht werden die Beziehungen zwischen den übergeordneten und den untergeordneten CIs dargestellt.
- Der Ereignis-Browser enthält eine Liste aller zugehörigen Ereignisse und zugehörigen Informationen in einer Tabellenansicht.
- In der Zustandstopologieansicht eines ausgewählten Ereignisses werden die zentralen Leistungsindikatoren (Key Performance Indicators, KPIs) des CI zu diesem Ereignis und die CIs in seiner Nachbarschaft angezeigt.

- Der Bereich "Zustandsindikatoren" enthält detaillierte Informationen zum Status des CI, das im Bereich "Zustandstopologieansicht" ausgewählt wurde. Diese Ansicht enthält Informationen zu den Leistungs-KPIs, Verfügbarkeits-KPIs und allen Zustandsindikatoren, die für das ausgewählte CI relevant sind.
- Im Bereich **Aktionen** werden die verfügbaren Aktionen für das ausgewählte Ereignis, das zugehörige CI oder den Knoten, auf dem das CI gehostet wird, angezeigt. Zu den Aktionen gehören Werkzeuge, Runbooks, benutzerdefinierte Aktionen und Leistungsdiagramme.

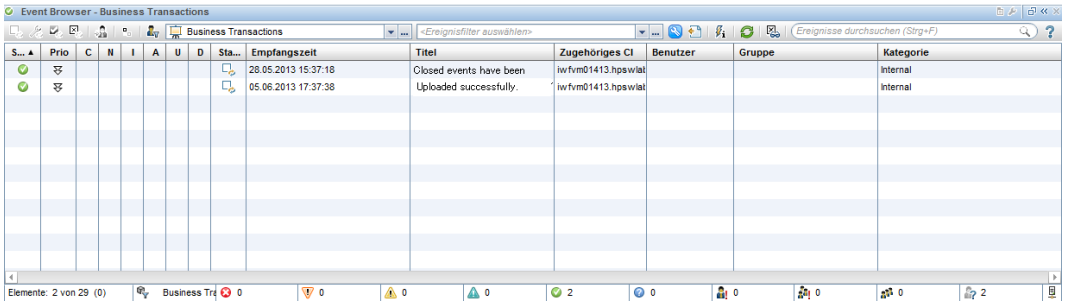
Ereignis-Browser

Der Ereignis-Browser ist der Bereich, auf den Dave zuerst schaut. Angezeigt werden:

- Eine Liste der priorisierten aktiven Ereignisse.
- Ereignisse, die ihm zugewiesen wurden.
- Informationen zu nicht aufgelösten und nicht zugewiesenen Ereignissen.
- Details, die zeigen, wie viele Ereignisse kritisch, wichtig, unbedeutend, Warnungen oder normal sind oder deren Status unbekannt ist.

Abbildung 8 unten zeigt eine typische globale Ansicht mit Ereignisinformationen im Bereich "Ereignis-Browser".

Abbildung 8 – Ereignis-Browser



Dave verwendet Filter, um Ereignisse in vordefinierten Ansichten anzuzeigen. Er kann aber auch seinen Arbeitsbereich personalisieren, indem er Filter und Registerkarten anpasst. Zum Beispiel kann er eine Kombination aus Schweregrad und Priorität verwenden, um die Ereignisse zu identifizieren, um die er sich sofort kümmern muss. Die erste Aufgabe besteht darin, festzustellen, welche der Ereignisse mit der höchsten Priorität zuerst untersucht werden müssen.

Zustandstopologieansicht

Wenn Dave ein Ereignis für die Untersuchung auswählt, wird die Zustandstopologieansicht aktualisiert und zeigt dann weitere Informationen zum zugehörigen CI an. Als Beispiel soll ein Ereignis dienen, das durch ein überschrittenes Speicherkontingent auf einem zugehörigen Server verursacht wurde. In der Zustandstopologieansicht wird die Topologieansicht des betroffenen Servers angezeigt. Dave kann ihn in dieser Ansicht auswählen, um weitere Informationen zu erhalten. Abbildung 7 auf Seite 32 zeigt eine typische Zustandstopologieansicht mit Geschäftsservices und CIs.

Abbildung 9 – Zustandstopologieansicht

Für jeden Knoten in der Zustandstopologieansicht kann er ein Kontextmenü verwenden, um Informationen zu den geschäftlichen Auswirkungen zu erhalten. Wenn er zum Beispiel Server7 auswählt, kann er sehen, welche Geschäftsservices oder Vereinbarungen zum Servicelevel (Service Level Agreements, SLAs) durch ein Ereignis oder einen Ausfall betroffen sein könnten. In der Zustandstopologieansicht kann ein Operator den Zustand jedes CI im Topologiediagramm sehen. Eine Untersuchung der vorgeschalteten und nachgeschalteten CIs könnte weitere Anhaltspunkte liefern, die helfen könnten, das Problem zu isolieren.

Der nächste Schritt ist die Ursachenanalyse im Bereich "Zustandsindikatoren".

Bereich "Zustandsindikatoren"

Wenn Dave das betroffene CI in der Zustandstopologieansicht auswählt, wird der Bereich "Zustandsindikatoren" aktualisiert und zeigt dann weitere Informationen zu diesem CI an. Die Trendspalte (siehe Abbildung 10 unten) zeigt, ob der aktuelle Status eine Verbesserung oder eine Verschlechterung gegenüber den Statusindikatoren aus der Vergangenheit bedeutet.

Abbildung 10 — Bereich "Zustandsindikatoren"

In dieser detaillierten Ansicht kann gezeigt werden, ob es ein zugrunde liegendes Problem gibt oder mehrere unterschiedliche Faktoren zum kritischen Ereignis beigetragen haben. Mit diesen Informationen kann Dave schneller entscheiden, was er als nächstes zu tun hat. Sobald er handelt, sehen andere Operatoren, dass Dave an diesem Problem arbeitet und können sich auf andere kritische Ereignisse konzentrieren.

Dave kann auch Leistungsdiagramme und weitere Werkzeuge verwenden, um das Problem zu beheben.

Sonstige Werkzeuge

Die Details eines Ereignisses können auch Anweisungen enthalten. Dave kann die Registerkarte **Zusätzliche Informationen** auswählen, die Hinweise oder weitere Tipps zur Lösung des Problems enthalten kann. Es könnte ein Diagnosewerkzeug oder -skript vorhanden sein, das er ausführen kann, um die Leistung von CIs sehr detailliert zu analysieren, oder zugehörige Protokolle mit informativen Fehlermeldungen.

Dave hat eigene Leistungsdiagramme zur Verfügung, die nützliche Analysewerkzeuge sind. Wenn zum Beispiel ein Datenbankleistungsereignis auftritt, kann Dave mit der rechten Maustaste auf das Ereignis klicken und **Anzeigen > Leistungsdiagramme (Nachbarschaft)** auswählen. Für das durch das Ereignis betroffene CI und seine benachbarten CIs, wie zum Beispiel den betroffenen Applikationsserver, werden Leistungsdiagramme angezeigt. Diese Diagramme zeigen nicht nur die Informationen zur Leistung zum Zeitpunkt des Ereignisses sondern auch die Leistung zu einem früheren Zeitpunkt.

Hinweis: Die BSM-Operationenverwaltungs-Werkzeuge können nicht nur zum Behandeln von Ereignissen verwendet werden. Dave kann solche Werkzeuge auch starten, um tägliche Routineaufgaben zu erfüllen.

Auflösung

Es gibt mehrere Möglichkeiten, ein Problem zu lösen. Bei diesem Beispiel sieht Dave einen Vorschlag, ein Werkzeug über das Menü **Starten** auszuführen. Dave klickt im Ereignis-Browser mit der rechten Maustaste auf das Ereignis und wählt **Starten > Werkzeuge > Dateisystem reparieren (CI)** aus. Wenn das Werkzeug beendet ist, ist das Problem behoben und das Ereignis verschwindet aus der Liste. Wenn dies nicht funktioniert, kann Dave im Bereich **Aktionen** auf zugehörige Runbooks zugreifen. Runbooks sind Skripts, die einen aus mehreren Schritten bestehenden Prozess zur Behebung des Problems ausführen.

Sonstige Rollen

Der Operator stützt sich auf die Fachkompetenz von zwei weiteren wichtigen Rollen:

- Der Entwickler von Überwachungslösungen

  Informationen hierzu finden Sie unter "Workflow des Entwicklers von Überwachungslösungen" auf Seite 39.

- Der Systemadministrator

  Informationen hierzu finden Sie unter "Workflow des Systemadministrators im Bereich IT-Betrieb" auf Seite 43.

Workflow des Entwicklers von Überwachungslösungen

Mike ist Entwickler von Überwachungslösungen auf der Basis der BSM-Operationenverwaltung. Seine Hauptaufgabe ist das Anpassen der BSM-Operationenverwaltung an spezielle Geschäftsanforderungen.

In der Regel integriert Mike neue Applikationen und CIs in den Überwachungsprozess. Zum Erstellen einer den Unternehmensstandards entsprechenden Überwachungsumgebung für zusammengesetzte Applikationen und Services konfiguriert Mike Monitoring Automation-Elemente, beispielsweise Managementvorlagen and Aspekte, und implementiert die technischen Überwachungsdetails, indem er Richtlinienvorlagen anpasst und sie mit Managementvorlagen und Aspekten verknüpft. Er macht die Überwachungslösungen zudem von Instanzen und Plattformen unabhängig, indem er automatische Zuweisungen und die bedingte Bereitstellungen von Aspekten verwendet.

Zum Beispiel muss er definieren, wie eine neue Gruppe Server, die FTP unterstützen, überwacht wird. Diese Server unterstützen kritische Geschäftsservices, indem sie es internen Abteilungen und Services ermöglichen, große Datenblöcke zu senden und zu empfangen.

Zuerst überträgt die Abteilung für Lohn- und Gehalt die entsprechenden Mitarbeiterinformationen von ihrem Server an die Lohnbuchhaltung des Unternehmens. Die Lohnbuchhaltung sendet dann interne Übersichtsreports (gesetzlich vorgeschriebene Berichte, die archiviert und an die zuständigen Behörden weitergegeben werden müssen) zurück und liefert weitere lohn- und gehaltsbezogene Daten.

Mike muss definieren, wie die FTP-Server überwacht werden sollen, um ihren störungsfreien Betrieb zu gewährleisten, muss sicherstellen, dass sie Anforderungen verarbeiten können, und muss FTP-Downloads in einer sicheren Umgebung ermöglichen. Wenn die Server nicht verfügbar sind, werden Termine nicht eingehalten, und in Extremfällen könnten nach einem Ausfall Geldstrafen wegen der Nichteinhaltung gesetzlich vorgeschriebener Anforderungen fällig werden.

Erstanalyse

Die ersten Dinge, an die Mike denken muss, sind die KPIs und die Zustandsindikatoren für FTP-Server. Es müssen einige wichtige Fragen beantwortet werden:

- Wenn Verfügbarkeit und Leistung von Applikationen wichtig sind, wie sollte er dann diese KPIs messen?

- Welche Vereinbarungen zum Servicelevel (Service Level Agreements, SLAs) würden verletzt, wenn die Schwellenwerte zur Verfügbarkeit und Leistung für einen FTP-Server nicht eingehalten werden?

Die IT-Organisation ist nicht nur für die Gewährleistung der Verfügbarkeit dieses Servers und der auf ihm befindlichen Applikationen verantwortlich sondern auch dafür, dass alle zugehörigen Ressourcen die Erwartungen der Benutzer erfüllen. Alle diese Information muss Mike bei seiner Auswahl der KPIs und der Definition der wichtigsten Zustandsindikatoren berücksichtigen.

Zustandsindikatoren definieren

Welche KPIs sollten im Überwachungsprozess gemessen werden?

Wie sollten sie zurück an die Eigner von Geschäftsservices gemeldet werden, die den FTP-Server nutzen?

Mike wendet sich der Definition der Zustandsindikatoren zu, die die ausgewählten KPIs unterstützen. Zum Beispiel könnten zu den Zustandsindikatoren für die Verfügbarkeit der Applikationen auf einem Windows-FTP-Server auch Metriken für Windows-Dienste gehören, die die folgenden Informationen bereitstellen:

- Anzahl der ausgehenden Verbindungen aller Typen vom Dienst
- Anzahl der übertragenen Bytes pro Sekunde
- Serverantwortzeit

Mike muss den Überwachungsprozess konfigurieren, die Überwachungsrichtlinie erstellen und festlegen, wie der Status gemeldet werden soll.

Leider stehen ihm mehrere HP-Applikationen zur Verfügung, die diese Aufgaben unterstützen. Seine Erfahrung und sein gesamtes Wissen über diese Applikationen helfen ihm, für diese Aufgabe die beste Wahl zu treffen. Er könnte sich beispielsweise für eine HP Operations Manager-Agentenrichtlinie, für HP SiteScope oder für ein anderes HP-Überwachungswerkzeug entscheiden. Für jeden Zustandsindikator, den er auswählt, muss es ein Werkzeug geben, das den Status dieses Zustandsindikators melden kann.

Sonstige Aufgaben

Es gibt eine Vielzahl unterschiedlicher Aufgaben, die Mike erfüllen muss, um den Prozess zur Überwachung und Erhaltung des Zustands für den FTP-Server zu gestalten. Dazu zählen die folgenden Aufgaben:

- Erstellen von Diagrammen, in denen die gesammelten Metriken für den FTP-Server zusammengefasst sind, und Zuweisen dieser Diagramme zum CI-Typ "FTP-Server", damit sie automatisch angezeigt werden.
- Erstellen von BSM-Operationenverwaltungs--Werkzeugen, um den FTP-Server neu zu starten.
- Erstellen von mehreren operativen Runbooks. Zum Beispiel könnte Mike ein Runbook zum Löschen veralteter Dateien vom FTP-Server erstellen.
- Erstellen von Content Packs, die die Überwachungsartefakte enthalten.

- Erstellen von Korrelationsregeln, um bestimmte identifizierte Datenträgerprobleme zu bestimmten Problemen mit dem FTP-Server zuzuordnen.

Die Rolle von Mike ist sehr wichtig. Er sieht voraus, welche Metriken notwendig sind und wie sie erfasst werden, und definiert die zugehörigen Prozesse, um die Daten zu sammeln und Probleme zu lösen.

Sonstige Rollen

Mike, der Entwickler von Überwachungslösungen, integriert neue Applikationen und CIs in den Überwachungsprozess. Diese werden von Matthew, dem Systemadministrator im Bereich IT-Betrieb, für die Verwendung durch die Operatoren Dave und seine Kollegen konfiguriert. Er entwickelt außerdem Managementlösungen, die von Alice, der Applikationsspezialistin, und ihren Kollegen verwendet werden.

Einblicke in diese anderen Rollen erhalten Sie unter:

- Der Systemadministrator

  Informationen hierzu finden Sie unter "Workflow des Systemadministrators im Bereich IT-Betrieb" auf Seite 43.

- Der Operator

  Informationen hierzu finden Sie unter "Workflow des Operators" auf Seite 33.

- Die Applikationsspezialistin

  Informationen hierzu finden Sie unter "Workflow der Applikationsspezialistin" auf Seite 47.

Workflow des Systemadministrators im Bereich IT-Betrieb

Im Kapitel "Einführung in die BSM-Operationenverwaltung" haben Sie das Konzept der Operations Bridge kennen gelernt. Die BSM-Operationenverwaltung ist die Operations Bridge für eine vollständige BSM-Überwachungslösung und stellt einen zentralen Ort für das Ereignis- und Leistungsmanagement bereit. Die Operations Bridge ermöglicht das konsolidierte Betriebsmanagement (Operationenverwaltung) für die BSM-Umgebung.

Im Kapitel "Workflow des Operators" haben wir erfahren, dass die Operations Bridge eine vollständige Übersicht über alle operativen Ereignisse bereitstellt und damit bei Bedarf eine unmittelbare Reaktion ermöglicht. Damit die Operations Bridge effizient ausgeführt werden kann, muss sie konfiguriert und optimiert werden. Dies ist die Aufgabe von Mike, dem Systemadministrator im Bereich IT-Betrieb.

Matthew wirkt im Hintergrund und gestaltet von dort aus eine effiziente Überwachungsumgebung für die IT-Mitarbeiter. In seiner Rolle stellt er die kontinuierliche Wartung sicher, verwaltet Benutzer und Benutzerrollen und sucht nach Möglichkeiten zur Optimierung des Überwachungsprozesses. Er entwirft das operative System und implementiert täglich die Prozesse, die andere Benutzer verwenden. Seine Spezialität sind das Erstellen neuer Skripts und das Automatisieren von möglichst vielen Prozessen.

Matthew muss über eine genaue Kenntnis der Betriebsumgebung verfügen, verstehen, wie Applikationen voneinander abhängen, und eine Umgebung konfigurieren, die so effizient wie möglich ist.

Aufgaben im Rahmen der Installation und Konfiguration

Matthew verfügt über das Fachwissen, um die BSM-Operationenverwaltung und Monitoring Automation zu installieren und zu konfigurieren. In einem einfachen Szenario gäbe es eine Instanz von Monitoring Automation für Server, die mit der Operations Manager i-Ereignisverwaltung-Foundation installiert wird. In einem komplexen Szenario könnten mehrere Instanzen von Operations Manager i und der BSM-Operationenverwaltung in einer verteilten MoM-Umgebung ("Manager of Managers") vorhanden sein (siehe "Einführung in die BSM-Operationenverwaltung" auf Seite 9). In einer MoM-Bereitstellung muss Matthew für eine nahtlose umgebungsübergreifende Integration HP Operations Orchestration-Workflows, HP Network Node Manager i-Vorfälle (NNMi) und Business Process Monitor-Ereignisse integrieren.

Matthew aktiviert den Überwachungsprozess auch durch die Installation der erforderlichen Überwachungswerkzeuge wie Operation Agents und Sitescope.

Matthew installiert und pflegt Content Packs, die von Überwachungsrichtlinien verwendete Definitionen enthalten, z. B. Content Packs für Monitoring Automation.

Matthew installiert, falls erforderlich, auch den HP BSM Integration Adapter, um die Integration von Domänen-Managern von Drittanbietern, beispielsweise Microsoft System Center Operations Manager (SCOM), zu unterstützen.

Matthew hat die folgenden Verantwortlichkeiten:

- Überwachen der BSM-Installation
- Optimieren der Umgebung
- Optimieren der Infrastruktureinstellungen
- Konfigurieren von Benutzern und Benutzerrollen

Überwachen der BSM-Installation

Matthew hat das Fachwissen und Erfahrung mit dem Betriebsmanagement (Operationenverwaltung). Er weiß genau, wie die BSM-Komponenten, einschließlich der Operationenverwaltung, installiert und richtig konfiguriert werden. Er entwirft und beaufsichtigt den kompletten Prozess zur Installation der erforderlichen BSM-Komponenten und entscheidet, welche Applikationen in BSM integriert werden sollen. Zu diesen Applikationen gehören andere HP-Unternehmenslösungen und Applikationen von Drittanbietern, wie zum Beispiel Microsoft SCOM.

Die Komplexität entsteht durch die Integration mehrerer Infrastruktur- und Unternehmensgeschäftsapplikationen gemäß den ITIL®-Prinzipien (Information Technology Infrastructure Library). Dabei besteht das Ziel in der Einrichtung und Konfiguration autonomer Applikationen, die nahtlos miteinander zusammenarbeiten. Jede Applikation arbeitet unabhängig, kommuniziert aber effektiv mit anderen Applikationen.

Optimieren der Umgebung

Matthew konfiguriert alle verbundenen Server. Danach definiert er Regeln für die Weiterleitung von Ereignissen und Benachrichtigungen und entscheidet, wer die Ereignisbenachrichtigung erhalten soll. In einigen Fällen besteht die Reaktion auf ein Ereignis in der Verwendung der benutzerdefinierten Skripts, die Matthew identifiziert oder sogar selbst herstellt. Schließlich entwirft er auch den Prozess, der neue Ereignisse einer bestimmten Benutzergruppe zuweist. Dies sind regelbasierte Filter, mit denen sichergestellt wird, dass die BSM-Operationenverwaltung jedes Ereignis automatisch der richtigen Gruppe oder Person zuweist.

Optimieren der Infrastruktureinstellungen

Diese Einstellungen repräsentieren einen großen Bereich des erforderlichen Fachwissens. Wenn Matthew eine Einstellung ändert, muss er die dabei entstehenden Auswirkungen auf die Betriebsumgebung genau kennen. Wenn er zum Beispiel einschränkt, was in das Audit-Protokoll geschrieben wird, werden Details bestimmter Ereignisse weggelassen. Andere Einstellungen beschreiben weitere Aspekte der Umgebung (wie zum Beispiel den SSL-Zertifikatsserver), die Verwaltung zugehöriger Ereignisse und die Verwaltung doppelter Ereignisse.

Konfigurieren von Benutzern und Benutzerrollen

Matthew ist für das Definieren von Benutzerrollen und der Rechte und Einschränkungen für diese Rollen verantwortlich. Die Benutzerrolle ist eine allgemeine Methode, mit der mehreren Benutzern

dieselben Rechte zugewiesen werden können, anstatt jede Berechtigung gesondert zu konfigurieren. Wenn ein neuer Operator oder Entwickler von Überwachungslösungen sein Arbeit antritt, fügt Matthew ihn zum System hinzu und weist eine seiner vordefinierten Benutzerrollen zu, um automatisch dieselben Rechte und Einschränkungen zu erteilen, die jeder andere Benutzer mit dieser Benutzerrolle besitzt.

Sonstige Verantwortlichkeiten

Zu den sonstigen Verantwortlichkeiten gehören:

- Entscheiden, welche EPI-Skripts (Event Processing Interface, Ereignisverarbeitungsschnittstelle) zu vordefinierten Zeitpunkten ausgeführt werden sollen
- Definieren von benutzerdefinierten Aktionen

Ständige Aufgaben

Nach der Erstinstallation und -konfiguration sind die Nutznießer die Operatoren, deren Aufgabe es ist, die Ereignisse, die sie überwachen, zu verwalten. Mike stellt dem Operator Dave eine Umgebung bereit, die dessen tägliche Aufgaben vereinfacht und sicherstellt, dass Dave so schnell und effizient wie möglich auf kritische Ereignisse reagieren kann.

Nach der Erstkonfiguration erfolgt die Wartung automatisch, bis ein Benutzer eine Änderung benötigt. Die meisten Umgebungen müssen sich auch mit der Zeit ändern, um neuen Anforderungen gerecht zu werden. Mike, der Entwickler von Überwachungslösungen, könnte neue oder aktualisierte Content Packs senden, die Mike dann installieren muss. Während das Unternehmen wächst, muss Mike neue Benutzer hinzufügen und jedem von ihnen die geeignete Benutzerrolle und die geeigneten Berechtigungen zuweisen.

Mike kann auch an den täglichen Abläufen erkennen, dass er einige seiner ursprünglichen Modelle für die Weiterleitung von Ereignissen und für Benachrichtigungen überarbeiten muss. Wenn neue Situationen entstehen, entscheidet Mike, ob vorhandene Skripts verwendet oder neue Reaktionsmodelle erstellt werden sollen. Durch die Optimierung der Umgebung werden der Betrieb effizienter und die Überwachung effektiver.

Operations Bridge

Durch das Erfassen aller Infrastrukturoperationen, einschließlich der Applikationen, der dedizierten Server und der zugehörigen Software und Hardware unter einem IT-Dach ist es möglich, die für das Unternehmen definierten Service-Level-Ziele zu erfüllen. Die Aufgabe von Mike ist die Konfiguration dieser Hochleistungsumgebung und die Verwendung der BSM-Operationenverwaltung als Operations Bridge. Alle Komponenten wirken zusammen, um den Mitarbeitern die notwendigen internen Geschäftsservices und externen Kunden bestimmte Portal-Services oder Applikationen mit definierter Verfügbarkeit bereitzustellen. Stellen Sie sich eine Umgebung für internationales Banking vor, die reihenweise Server, Applikationen, CIs und mehr enthält, um zu 99,999 % eine Reaktion zu gewährleisten. Bei einer solchen Zusage ist eine klar strukturierte Betriebsumgebung der Art erforderlich, wie sie von Mike bereitgestellt wird.

Sonstige Rollen

Matthew, der Systemadministrator im Bereich IT-Betrieb, konfiguriert und optimiert die Operations Bridge, einschließlich der von Mike, dem Entwickler von Überwachungslösungen, entwickelten Inhalte, für die Verwendung durch die Operatoren Dave und seine Kollegen.

Einblicke in diese anderen Rollen erhalten Sie unter:

- Der Entwickler von Überwachungslösungen

  Informationen hierzu finden Sie unter "Workflow des Entwicklers von Überwachungslösungen" auf Seite 39.

- Der Operator

  Informationen hierzu finden Sie unter "Workflow des Operators" auf Seite 33.

Workflow der Applikationsspezialistin

Im Kapitel "Einführung in die BSM-Operationenverwaltung" haben Sie das Konzept der Operations Bridge kennen gelernt. Die BSM-Operationenverwaltung ist die Operations Bridge für eine vollständige BSM-Überwachungslösung und stellt einen zentralen Ort für das Ereignis- und Leistungsmanagement bereit. Die Operations Bridge ermöglicht das konsolidierte Betriebsmanagement (Operationenverwaltung) für die BSM-Umgebung.

Sie haben außerdem erfahren, wie Monitoring Automation dazu beitragen kann, eine flexible Überwachungslösung für Applikationen und Services zu erstellen.

Im Kapitel "Workflow des Entwicklers von Überwachungslösungen" haben wir Mike kennen gelernt, der Überwachungslösungen entwickelt, die mit den Unternehmensrichtlinien zu Überwachungsinhalten und -verfahren in Einklang stehen.

Alice ist Applikationsspezialistin für eine bestimmte Anwendung oder einen bestimmten Service. Sie ist diejenige Person, die am meisten über die Systeme, auf denen die Applikation ausgeführt wird, und die Art ihrer Verwendung weiß. Alice ist für die Bereitstellung der von Mike entwickelten Managementvorlagen verantwortlich, um die eigentliche Applikationsinstanz zu überwachen, für die sie verantwortlich ist.

Aufgaben im Rahmen der Installation und Konfiguration

Bevor sie mit der Überwachung des Systems beginnt, optimiert Alice die Werte im Hinblick auf die zu überwachende Applikation. Die Werte, die Mike, der Entwickler, in den Managementvorlagen konfiguriert hat, spiegeln die unternehmensweiten Standards für die Überwachung von Applikationen des Typs wider, zu dem auch die von Alice betreute Applikation gehört. Alice muss einige dieser Werte möglicherweise ändern, damit sie zu der Applikationsinstanz passen, für die sie verantwortlich ist.

Nachdem sie die Managementvorlage optimiert hat, weist sie sie zu und stellt sie bereit.

- Die Operationenverwaltung ermittelt Instanzen der CI-Typen in der Topologieansicht, die in der Managementvorlage konfiguriert wurden. Alice muss nur noch die automatischen Zuweisungen definieren, die für die Managementvorlage vorgenommen werden können. Nachdem die automatischen Zuweisungen für die Managementvorlage konfiguriert wurden, gleicht die Operationenverwaltung die CI-Typen in der Managementvorlage mit den ermittelten CI-Instanzen ab und stellt die Aspekte bereit, die für die automatische Überwachung erforderlich sind.

- Wenn mehr Kontrolle erforderlich ist, kann Alice die Managementvorlage oder den Aspekt manuell zu ermittelten CIs zuweisen. Danach stellt die Operationenverwaltung die Aspekte in der Managementvorlage bereit.

Ständige Aufgaben

Während der Überwachungsprozess ausgeführt wird, prüft Alice von Zeit zu Zeit die Bereitstellungsjobs für die Applikation, um sicherzustellen, dass der Überwachungsprozess ordnungsgemäß ausgeführt wird.

Falls die von Alice betreute Applikation ein Ereignis generiert, kann sie applikationsspezifische Tools aus der OMi-Konsole einsetzen, um die Probleme zu beheben.

Sonstige Rollen

Alice, die Applikationspezialistin, optimiert und initiiert den Überwachungsprozess für die Applikationsinstanz, für die sie verantwortlich ist, mithilfe einer Managementvorlage, die von dem Entwickler Mike entwickelt wurde. Der Überwachungsprozess generiert Ereignisse, die von Dave, dem Operator behandelt werden.

Einblicke in diese anderen Rollen erhalten Sie unter:

- Der Entwickler von Überwachungslösungen

  Informationen hierzu finden Sie unter "Workflow des Entwicklers von Überwachungslösungen" auf Seite 39.

- Der Operator

  Informationen hierzu finden Sie unter "Workflow des Operators" auf Seite 33.

Zusammenfassung

Nachdem Sie etwas über die unterschiedlichen Benutzer erfahren haben, die die täglichen Prozesse der BSM-Operationenverwaltung installieren, konfigurieren und verwalten, wissen Sie, dass Know-how auf mehreren Gebieten erforderlich ist, damit alles optimal läuft. Möglicherweise arbeiten auch Sie in einer der Rollen, die in diesem Handbuch beschrieben sind. Unabhängig von der Rolle, die Sie übernehmen, können Sie Ihren Beitrag dazu leisten, wie gut Ihre Arbeitsgruppe Ihren internen Kunden einen Nutzen bereitstellt.

Index


Java™
COMPATIBLE