

HP Business Service Management

für Windows® und Linux

Softwareversion: 9.20

Operations Manager *i* Konzepthandbuch

Dokument-Releasedatum: August 2012
Software-Releasedatum: August 2012



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 US-Regierung per Standardlizenz lizenziert.

Urheberrechtshinweise

© Copyright 2008-2012 Hewlett-Packard Development Company, L.P.

Marken

Adobe® und Acrobat® sind Marken der Adobe Systems Incorporated.

AMD und das AMD Arrow-Logo sind eingetragene Marken von Advanced Micro Devices, Inc.

Google™ und Google Maps™ sind eingetragene Marken von Google Inc.

Intel®, Itanium®, Pentium® und Intel® Xeon® sind eingetragene Marken der Intel Corporation in den Vereinigten Staaten und anderen Ländern.

iPod ist eine Marke der Apple Computer, Inc.

Java ist eine eingetragene Marke von Oracle und/oder der zugehörigen Tochtergesellschaften.

Microsoft®, Windows®, Windows NT®, Windows® XP und Windows Vista® sind in den Vereinigten Staaten eingetragene Marken der Microsoft Corporation.

Oracle ist eine eingetragene Marke der Oracle Corporation und/oder der zugehörigen Tochtergesellschaften.

UNIX® ist eine eingetragene Marke von The Open Group.

Hinweise

Dieses Produkt beinhaltet Software, die von Apache Software Foundation entwickelt wurde (<http://www.apache.org>).

Dieses Produkt beinhaltet Software, die vom JDOM-Projekt entwickelt wurde (<http://www.jdom.org/>).

Dieses Produkt beinhaltet Software, die vom MX4J-Projekt entwickelt wurde (<http://mx4j.sourceforge.net>).

Dokumentationsaktualisierungen

Die Titelseite dieses Dokuments enthält die folgenden bezeichnenden Informationen:

- Software-Versionsnummer zur Angabe der Software-Version.
- Dokument-Releasedatum, das sich mit jeder Aktualisierung des Dokuments ändert.
- Software-Releasedatum zur Angabe des Releasedatums der Software-Version.

Um nach Aktualisierungen des Dokuments zu suchen oder um zu überprüfen, ob Sie die aktuellste Version des Dokuments verwenden, wechseln Sie zu:

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

Für die Anmeldung an dieser Website benötigen Sie einen HP Passport. Um sich für eine HP Passport-ID zu registrieren, wechseln Sie zu:

<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.

Unterstützung

Besuchen Sie die HP Software Support Online-Website unter:

www.hp.com/go/hpsoftwaresupport

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

Die Onlineunterstützung von HP Software bietet den Kunden Möglichkeiten, Probleme selbst zu lösen. Sie bietet schnelle und effiziente Wege, auf interaktive Werkzeuge für den technischen Support zuzugreifen, die für die Führung des Unternehmens erforderlich sind. Als Kunde mit Supportvertrag stehen Ihnen beim Support folgende Optionen zur Verfügung:

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

Bei den meisten Support-Bereichen ist die Registrierung und Anmeldung als HP-Passport-Benutzer erforderlich. Einige Angebote setzen den Abschluss eines Supportvertrags voraus. Um sich für eine HP Passport-ID zu registrieren, wechseln Sie zu:

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

Weitere Informationen zu den Zugriffsebenen finden Sie unter:

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

Inhalt

1	Willkommen	7
	Aufbau dieses Handbuchs	7
	Wer dieses Handbuch lesen sollte	7
2	Einführung in die BSM-Operationenverwaltung	9
	Lizenzstruktur	9
	Operations Bridge für eine vollständige BSM-Lösung	10
	Datenübernahme aus mehreren Quellen	11
	Konsolidiertes Ereignis- und Leistungsmanagement	12
	Ereignisinformationen	12
	Ereignis-Dashboards	13
	Zustandsinformationen	14
	Korrelieren von Ereignissen	15
	Unterdrücken doppelter Ereignisse	15
	Automatisches Schließen zugehöriger Ereignisse	16
	Stream-basierte Ereigniskorrelation	16
	Topologiebasierte Ereigniskorrelation	16
	Ereignis-Storm-Unterdrückung	17
	Strukturierte Problemlösung	18
	Verwalten von Inhalten mit Content Packs	20
	Vordefinierte Content Packs	21
	Werkzeuge zur Verwaltung von Inhalten	22
	Skalierbare Architektur mit mehreren Servern	22
	Manager-of-Managers	24
	Integrationsschnittstellen	25
	Benutzerrollen und Verantwortlichkeiten	26
3	Workflow des Operators	29
	Die Umgebung des Operators	31
	Zustandsperspektive	31
	Ereignis-Browser	32
	Zustandstopologieansicht	32
	Ausschnitt "Zustandsindikatoren"	33
	Sonstige Werkzeuge	34
	Auflösung	34
	Sonstige Rollen	35
4	Workflow des Entwicklers von Überwachungslösungen	37
	Erstanalyse	37
	Zustandsindikatoren definieren	38

Sonstige Aufgaben	38
Sonstige Rollen	39
5 Workflow des Systemadministrators im Bereich IT-Betrieb	41
Aufgaben im Rahmen der Installation und Konfiguration	41
Die BSM-Installation überwachen	42
Die Umgebung optimieren	42
Infrastruktureinstellungen optimieren	42
Benutzer und Benutzerrollen konfigurieren	43
Sonstige Verantwortlichkeiten	43
Ständige Aufgaben	43
Operations Bridge	43
Sonstige Rollen	44
Übersicht	44

1 Willkommen

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

- ▶ Die BSM-Operationenverwaltung ist in einer Bereitstellung von HP Business Service Management (BSM) mit aktiver Operations Manager *i*-Lizenz (OMi-Lizenz) verfügbar (siehe [Lizenzstruktur](#) auf Seite 9).

Weitere Informationen zur Bereitstellung finden Sie im *HP Business Service Management – Handbuch zur Bereitstellung*.

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 29:
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 37:
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 41:
Eine Beschreibung, wie die Rolle von Matthew aussieht und wie er die BSM-Operationenverwaltung-Umgebung überwacht und die Betriebsinfrastruktur so konfiguriert, dass alle Applikationen und Server in seiner Domäne integriert werden.

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

Wenn Sie einer dieser Benutzer sind, sind Sie sicher mit BSM und den grundlegenden Konzepten der Überwachung und des Managements in Unternehmen vertraut.

2 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](#) auf Seite 9

[Operations Bridge für eine vollständige BSM-Lösung](#) auf Seite 10

[Konsolidiertes Ereignis- und Leistungsmanagement](#) auf Seite 12

[Strukturierte Problemlösung](#) auf Seite 18

[Verwalten von Inhalten mit Content Packs](#) auf Seite 20

[Skalierbare Architektur mit mehreren Servern](#) auf Seite 22

[Integrationsschnittstellen](#) auf Seite 25

[Benutzerrollen und Verantwortlichkeiten](#) auf Seite 26

Lizenzstruktur

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

Weitere Informationen zur Bereitstellung finden Sie im *HP Business Service Management – Handbuch zur Bereitstellung*.

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

- **Ereignisverwaltung-Foundation**

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

Operations Bridge für eine vollständige BSM-Lösung

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

Die BSM-Operationenverwaltung verknüpft das Infrastrukturmanagement mit dem Management von Applikationen und Geschäftsservices. Sie kombiniert Ereignisse aus HP Business Service Management-Komponenten, z. B. Business Process Monitor (BPM), Real User Monitor (RUM) und Service Level Management (SLM), mit Ereignissen aus den Operationenverwaltungs-Komponenten der BSM-Lösung, z. B. 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 zeigt ein Beispiel für eine typische Bereitstellung, bei der die BSM-Operationenverwaltung die Operations Bridge in einer BSM-Lösung ist. Die BSM-Operationenverwaltung ermöglicht die automatisierte Überwachung und Integration von mehreren externen Applikationen und wird in der BSM-Plattform unter Verwendung der einheitlichen RTSM-Datenbank (RTSM = Run-Time Service Model) ausgeführt.

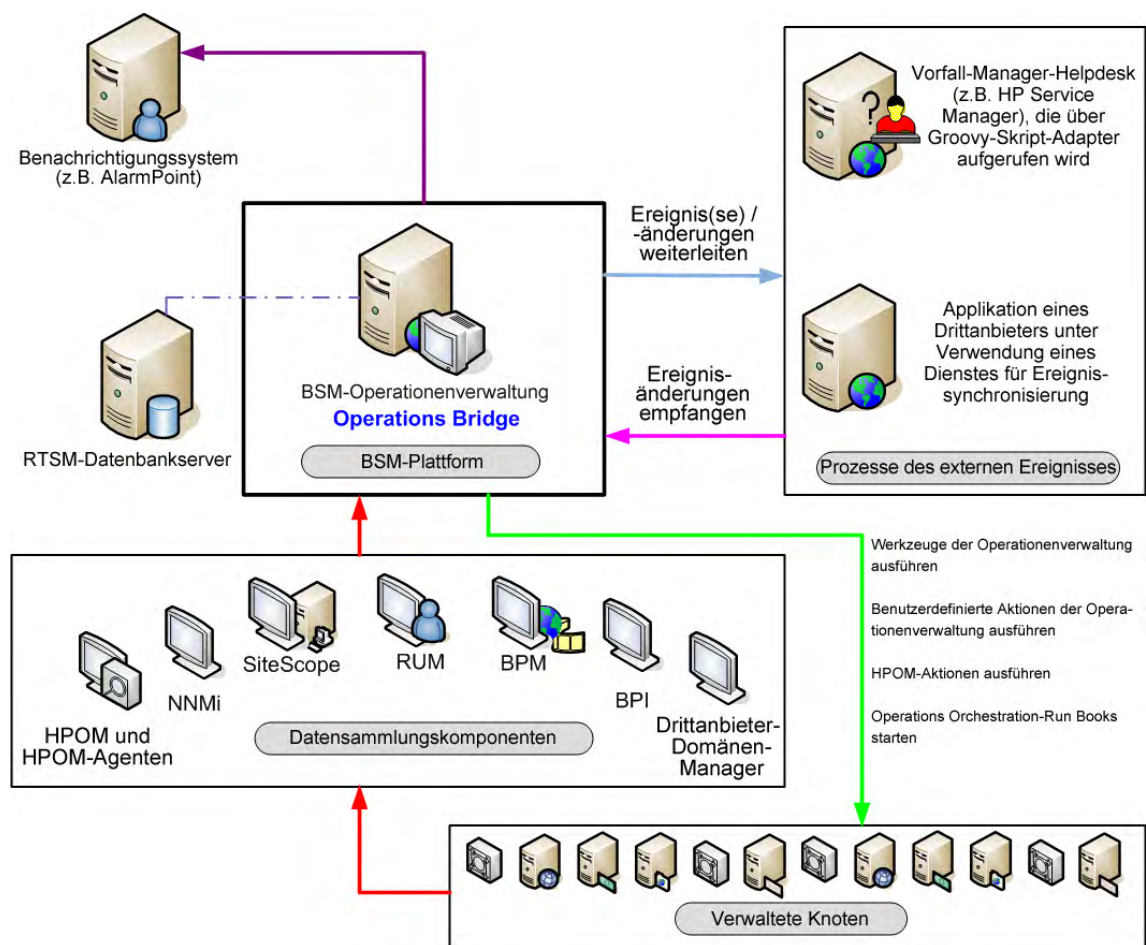


Abbildung 1 Operations Bridge in einer BSM-Lösung

Die gemeinsame Nutzung von RTSM mit anderen BSM-Applikationen bedeutet, dass immer ein direkter Zugriff auf die neuesten Daten in RTSM möglich ist. Dadurch entsteht für Systemadministratoren im Bereich IT-Betrieb kein zusätzlicher Aufwand bei der Verwaltung der Topologiedaten in 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 Seite 11 zeigt, werden Ereignisse ungeachtet dessen, woher sie stammen, auf einheitliche Art und Weise verarbeitet und verwaltet.

Beispiele für Ereignisquellen:

- 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 for Windows (HPOM for 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 Operationverwaltung weitergeleitet und dann zugehörigen Konfigurationselementen (Configuration Items, CIs) in 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 Datenerfassungsmodule (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 Zustand von Ereignissen und Nachrichten. Wenn ein BSM-Operationenverwaltung-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 bieten auf einen Blick eine Übersicht über die Ereignisse aus Ihrer 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.

The screenshot displays the Business Service Management Operations Management interface. The main dashboard area contains several widgets: 'Unassigned High Priority', 'Unassigned Events' (highlighted with a red box), 'Unresolved > 1 hour', 'Unresolved > 3 hours', 'Overall' (with a pie chart), and 'Business related'. A red arrow points from the 'Unassigned Events' widget to the 'Ereignis-Browser für Dashboard Widget Overall' window at the bottom. This window shows a table of events with columns for severity (Schw), priority (Prío), status (C, N, I, A, U, D, St), reception time (Empfangszeit), title (Titel), associated CI (Zugehöriges CI), user (Benutzer), and group (Gruppe). The events listed include 'Insufficient disk space' and 'Auto Upload of content finished'.

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 2 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.

The screenshot displays the Business Service Management (BSM) Operations Management interface. The main window is titled "Event Perspective" and shows a table of events. The table has columns for "Schw", "C", "N", "I", "A", "U", "D", "Titel", "Zugehöriges CI", "Status", "Benutzer", and "Gruppe". The "Titel" column contains various event descriptions, such as "Modified by CA/EP: Daily synchronization of agent services" and "Daily synchronization of agent services failed". The "Zugehöriges CI" column lists various CI identifiers like "j0b", "Server7", "j0b", "administrator", "Stefan", and "A-Tr".

Below the main window, there are several panels:

- Model Explorer:** Shows a hierarchical tree structure of objects, including "OprSample", "Gold ESS", "Employee Self Service", "ESS-0a", "ESS-0b", "ITBoss Cluster", and "serv0".
- Health Top View:** Shows a diagram of the state topology, with nodes representing different components and their relationships.
- Health Indicators:** Shows a table of health indicators for the selected CI, with columns for "Health Indicator", "Status", and "Wert".
- Actions:** Shows a list of actions that can be performed on the selected CI, such as "Show Performance Graph...", "Restart Windows Server (CI)", "Restart Windows Server (Knoten)", "Search Bino", "Search Google", and "Show event de...".

Red boxes highlight specific areas in the screenshot:

- "Model Explorer" is highlighted in the top-left panel.
- "Ereignis-Browser" is highlighted in the main event table.
- "Ausschnitt 'Zustandstopologieansicht'" is highlighted in the Health Top View panel.
- "Ausschnitt 'Zustandsindikatoren'" is highlighted in the Health Indicators panel.
- "Ausschnitt 'Aktionen'" is highlighted in the Actions panel.

Abbildung 2 Zustandsperspektive mit den Ausschnitten "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. Wenn es auch wichtig ist, die Anzahl der angezeigten Ereignisse im Ereignis-Browser zu minimieren, so ist es dadurch noch wichtiger, die Ereignisse hervorzuheben, die unbehandelt 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.

BSM Die 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 verglichen. 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 Serienergebnissen:** 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 Ursachenergebnis 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 Ursachenergebnisses 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-Sturm-Unterdrückung

Ein Ereignis-Sturm 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-Stürmen auf verwalteten Systemen gesucht wird und alle nachfolgenden Ereignisse verworfen werden, bis die Ereignis-Sturm-Bedingung für ein bestimmtes System nicht mehr besteht.

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

Wenn auf einem System ein Ereignis-Sturm erkannt wird, werden die Ereignisse auf diesem System verworfen, bis die Rate der eingehenden Ereignisse wieder unter den Ereignis-Sturm-Schwellenwert fällt. Sie können Ausnahmeregeln konfigurieren, um Ereignisse auf einem System, auf dem zurzeit ein Ereignis-Sturm 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 Skripten mit Beispielskripten, 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 in der 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 HP Operations Orchestration (OO) verwenden, um Operatortätigkeiten der Problemanalyse oder Problemlösung zu automatisieren, können diese OO-Runbooks bestimmten CI-Typen in BSM zugeordnet werden. Die OO-Runbooks können Sie in einem Ereigniskontext in 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 Gruppen mit den Operatoren, die für das Auflösen dieser Ereignisse verantwortlich sind, zugewiesen werden.
- 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 Skripten 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 einfließen lassen, indem Sie Ereignisse mit Tipps und Hinweisen zur Verbesserung des Verständnisses und zur Erklärung des dem Ereignis zugrunde liegenden Problems versehen.

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 speziellen CI-Daten für die BSM-Operationenverwaltung werden in 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:

- Vordefinierte Content Packs zur Ergänzung der Daten, die zum Beispiel durch NNMi oder HP Operations Manager Smart Plug-ins (SPI) 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 3 enthält eine Übersicht über den Inhalt, der sich in einem Satz Content Packs befinden kann.

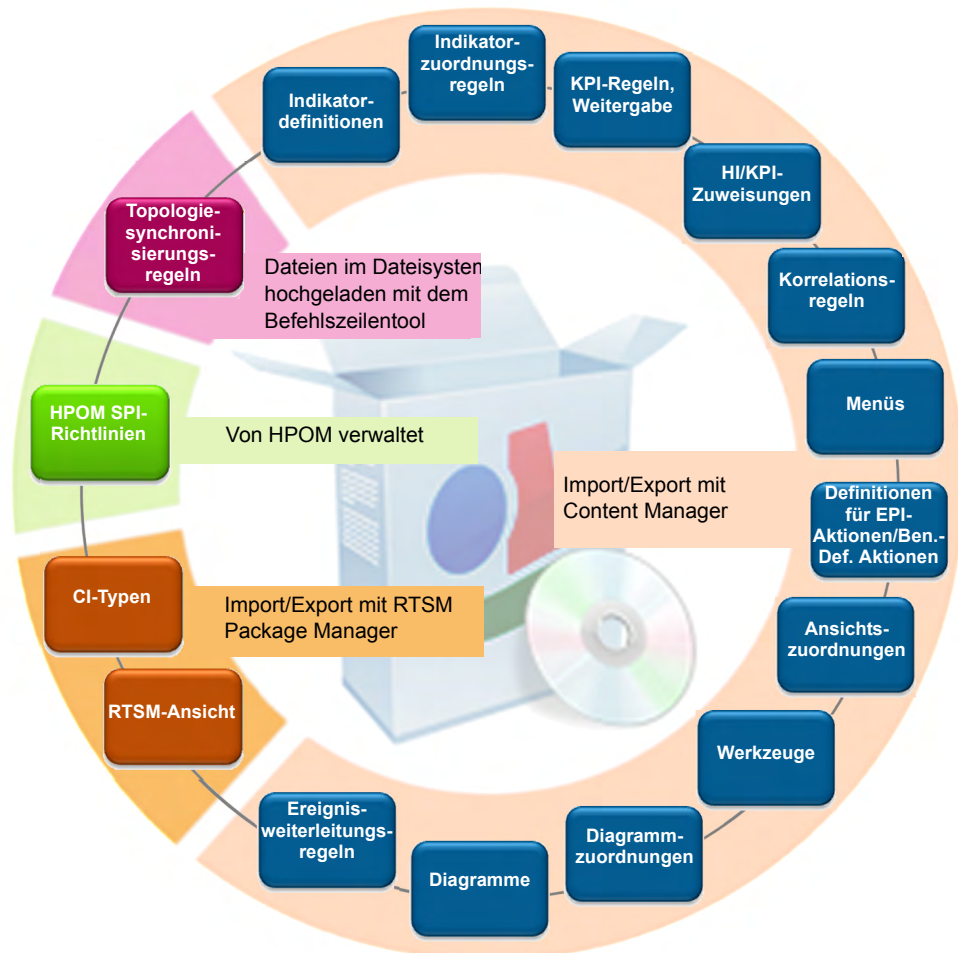


Abbildung 3 Der Inhalt kann sich in einem Satz Content Packs befinden.

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

BSM Die 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.

Bei der skalierbaren Architektur können eine oder mehrere Instanzen der BSM-Operationenverwaltung zu einer einzelnen leistungsstarken Managementlösung so kombiniert werden, dass sie die Anforderungen Ihrer Organisationsstruktur erfüllt. 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 betrieben wird, so konfiguriert werden, dass sie entweder nur mit anderen ähnlichen Servern oder aber 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 als zentrale Ereigniskonsole für die gesamte 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.

Server, auf denen die BSM-Operationenverwaltung betrieben wird, können Sie für die folgenden Zwecke konfigurieren:

- Für die Weiterleitung von Ereignissen an andere Server, auf denen die BSM-Operationenverwaltung betrieben wird, und für die Synchronisierung dieser Ereignisse zwischen den Servern.

- 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 den Servern, auf denen die BSM-Operationenverwaltung und HPOM-Management-Server betrieben werden.
- 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 4 zeigt ein Beispiel für eine hierarchische, verteilte Umgebung mit einem zentralen Server, auf dem die BSM-Operationenverwaltung betrieben wird und der nach dem Prinzip des serverbasierten flexiblen Managements andere regionale Server, auf denen BSM Operationenverwaltung betrieben wird, verwaltet.

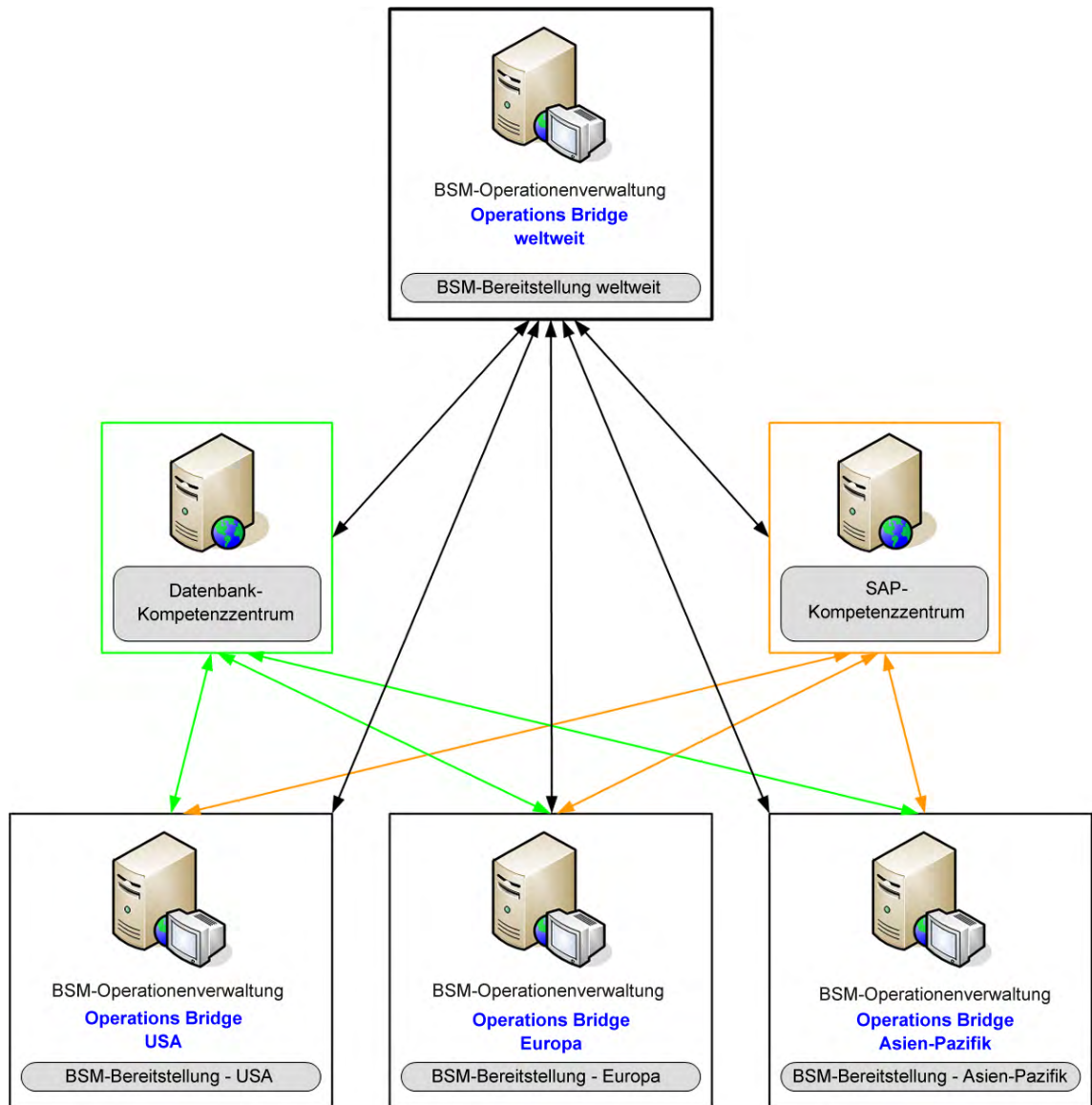


Abbildung 4 Manager-of-Managers-Implementierung (MoM)

In diesem Beispiel verwalten die Implementierungen auf den regionalen Servern BSM Europe, BSM USA und BSM Asia Pacific unterschiedliche Regionen. Die BSM-Operationenverwaltung in der Implementierung auf dem Server BSM Worldwide 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 das Spezialwissen 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 4** auf Seite 24 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.

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 Ereignisverarbeitungs-pipeline 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 eine 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 Ereignissynchronisierungsschnittstelle als Webservice 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 die Entwickler von Inhalten und die Integrationsverantwortlichen zur Anpassung und Erweiterung der Funktionalität der BSM-Operationenverwaltung.

Benutzerrollen und Verantwortlichkeiten

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

- Der Operator ist der praktische Ereignismanager und Problemlöser.
- Der Entwickler von Überwachungslösungen ist der Zustandsmanager, der entscheidet, was überwacht werden soll und welche Leistungsebenen geeignet sind.
- 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.

In [Tabelle 1](#) auf Seite 27 finden Sie häufig verwendete Titel für diese drei Benutzerrollen sowie eine Übersicht über ihre Verantwortlichkeiten. Nachdem wir mehr über die BSM-Operationenverwaltung wissen, begleiten wir in den folgenden Kapiteln drei typische Benutzer, um zu sehen, wie sie ihren Arbeitstag organisieren und ihre Aufgaben erfüllen.

Tabelle 1 Benutzerrollen

Stellenbezeichnung	Weitere Bezeichnungen	Verantwortlichkeiten
<p>Operator</p>  <p>"Dave"</p>	<ul style="list-style-type: none"> • Domänenoperator • Operator im Bereich IT-Betrieb 	<p>Überwacht täglich die Ereignisse, die ihm oder seiner Arbeitsgruppe zugewiesen wurden.</p> <p>Führt außerhalb der BSM-Operationenverwaltung Routineoperationen an den Applikationen, Systemen und Netzwerken, für die er verantwortlich ist, aus.</p> <p>Behebt Probleme mit Ereignissen, die zu einem Vorfall eskalieren könnten.</p>
<p>Entwickler von Überwachungslösungen</p>  <p>"Mike"</p>	<ul style="list-style-type: none"> • Fachmann • Entwickler von Überwachungslösungen im Bereich IT-Betrieb • Fachexperte für Applikationen, Netzwerke oder Spezialgebiete 	<p>Passt die Art und Weise an, in der die BSM-Operationenverwaltung eine Domäne überwacht.</p>
<p>Administrator</p>  <p>"Matthew"</p>	<ul style="list-style-type: none"> • Systemadministrator • Systemadministrator im Bereich IT-Betrieb • BSM Operationenverwaltungs-Administrator • Systemarchitekt 	<p>Überwacht die BSM-Operationenverwaltungs-Umgebung und Aufgabenzuweisungen. Integriert die BSM-Operationenverwaltung mit anderen Werkzeugen und Prozessen.</p>

In nächsten Kapitel erfahren wir mehr über die täglichen Verantwortlichkeiten des Operators Dave in einer Unternehmensumgebung mit der BSM-Operationenverwaltung als Operations Bridge.

3 Workflow des Operators



In Kapitel 2, Einführung in die BSM-Operationenverwaltung, haben wir Dave kennengelernt. Dave ist der Operator, der für das tägliche Management in einer BSM-Installation verantwortlich ist. Ein Operator ist in der IT-Umgebung eines Unternehmens in der Regel eine Stelle auf Einstiegsebene, aber Dave bringt bereits diverse Kompetenzen mit, da er bereits Erfahrung mit vielen der Technologien in der BSM-Operationenverwaltung-Umgebung besitzt.

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 BSM-Operationenverwaltung-Benutzeroberfläche 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 alle seine zustandsbezogenen

Werkzeuge nutzen muss. 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 es (unter Umständen einschließlich seiner Eigentümerschaft) an eine externe Ereignisverarbeitungsapplikation weiterleitet, zum Beispiel an einen HP Service Manager Helpdesk-Operator.

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

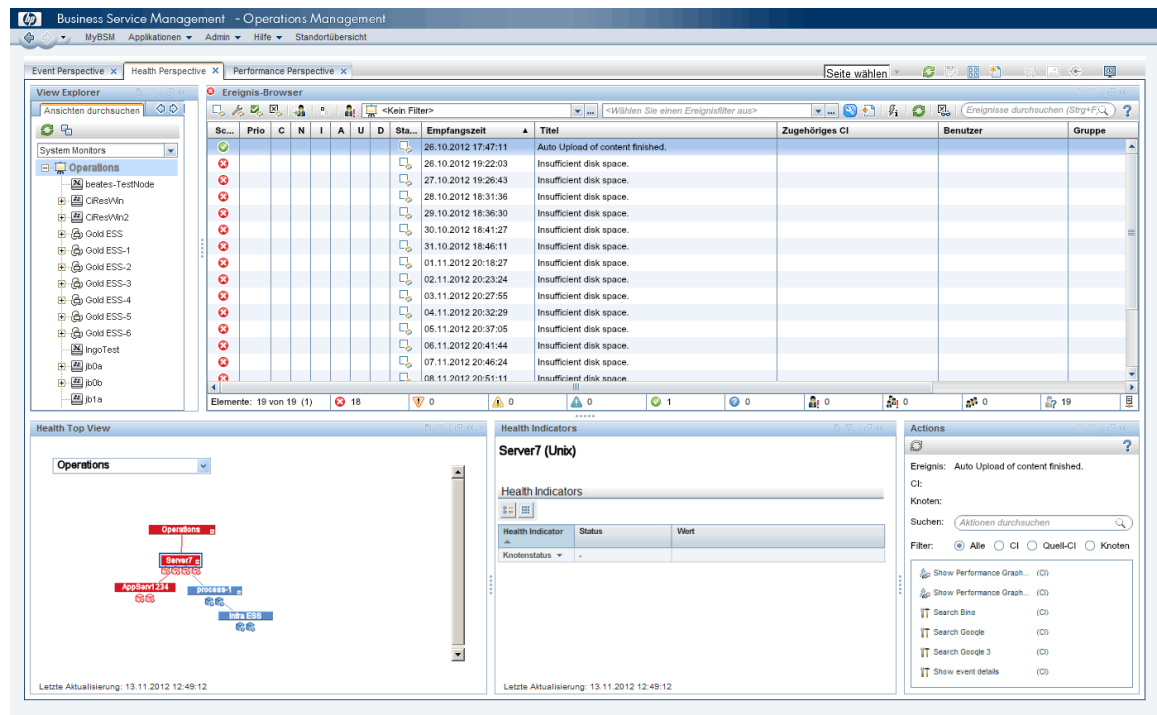


Abbildung 5 Zustandsperspektive

Die fünf Ausschnitte bieten eine globale Ansicht der Ereignisse im Bereich von Dave:

- 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 Ausschnitt "Zustandsindikatoren" enthält detaillierte Informationen zum Status des CI, das im Ausschnitt "Zustandstopologieansicht" ausgewählt wurde. Diese Ansicht enthält Informationen zu den Leistungs-KPIs, Verfügbarkeits-KPIs und Zustandsindikatoren, die für das ausgewählte CI relevant sind.
- Im Ausschnitt **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 6 zeigt eine typische globale Ansicht mit Ereignisinformationen im Ausschnitt "Ereignis-Browser".

Schw	C	I	A	U	D	Empfangszeit	Titel	Zugehöriges CI	Status	Benutzer	Gruppe
						07/04/2010 3:00:08 AM	Modified by CA/EPI: Daily synchronization of agent services	jb0b			
						07/03/2010 3:00:08 AM	Modified by CA/EPI: Daily synchronization of agent services	Server7			
						07/02/2010 2:59:55 AM	Modified by CA/EPI: Daily synchronization of agent services	jb0b			
						07/01/2010 2:59:36 AM	Modified by CA/EPI: Daily synchronization of agent services	jb0b			
						06/30/2010 2:59:36 AM	Modified by CA/EPI: Daily synchronization of agent services	jb0b			
						06/29/2010 2:59:47 AM	Modified by CA/EPI: Daily synchronization of agent services	jb0b			
					4	06/28/2010 3:00:10 AM	Daily synchronization of agent services failed ! (look at ann	jb0b		administrator	
						06/25/2010 11:29:35 AM	Modified by CA/EPI: Test DDDDDAAAAAAA	jb0b			
						06/25/2010 11:26:26 AM	Daily synchronization of agent services failed ! (look at ann	jb0b		Stefan	A-Te
						06/25/2010 11:26:03 AM	Modified by CA/EPI: Daily synchronization of agent services	jb0b			
						06/25/2010 11:26:46 AM	Modified by CA/EPI: Daily synchronization of agent services				
						06/25/2010 11:26:26 AM	TEst sdfjskifjskifjskifjskifjskifjskifjskifjskifjskifjskifjskifjskif			administrator	
						06/23/2010 2:09:48 PM	extending tablespace TS-ESS-0b failed	TS-ESS-0b			
						06/23/2010 2:09:42 PM	Modified by CA/EPI: Daily synchronization of agent services	jb0b		administrator	
						06/23/2010 9:26:37 AM	extending tablespace TS-ESS-0b failed	TS-ESS-0b		Stefan	A-Te
						06/23/2010 9:26:31 AM	extending tablespace TS-ESS-0b failed	TS-ESS-0b			
						06/21/2010 10:37:02 AM	Daily synchronization of agent services failed ! (look at ann	jb0b		administrator	
						06/18/2010 4:26:06 PM	I have an instruction	jb0b		administrator	

Abbildung 6 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 sie in seiner Ansicht auswählen, um weitere Informationen zu erhalten. [Abbildung 7](#) auf Seite 33 zeigt eine typische Zustandstopologieansicht von Geschäftsservices und CIs.

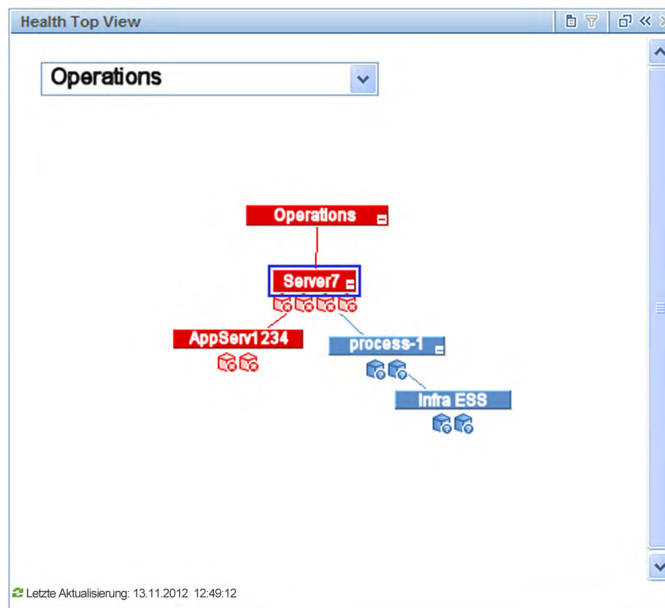


Abbildung 7 Zustandstopologieansicht

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 Ausschnitt "Zustandsindikatoren".

Ausschnitt "Zustandsindikatoren"

Wenn Dave das betroffene CI in der Zustandstopologieansicht auswählt, wird der Ausschnitt "Zustandsindikatoren" aktualisiert und zeigt dann weitere Informationen zu diesem CI an. Die Trendspalte (siehe [Abbildung 8](#) auf Seite 34) zeigt, ob der aktuelle Status eine Verbesserung oder eine Verschlechterung gegenüber den Statusindikatoren aus der Vergangenheit bedeutet.

KPI	Health Indicator	Status	Letzte Statusänderung	Trend
System Availability	Storage	⊗ Critico	7/20/10 5:11 PM	↕
	Node state	⊗ Inactivo	7/20/10 5:18 PM	↕
System Performance	CPU	⊗ Critico	7/19/10 4:30 PM	↕
	Memory	⊗ Inactivo	7/19/10 4:30 PM	↕

Letzte Aktualisierung: 12.11.2012 14:59:53

Abbildung 8 Ausschnitt "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: BSM Operationenverwaltung-Werkzeuge sind nicht auf die Behebung von Fehlern bei Ereignissen beschränkt. 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 den Vorschlag zur Ausführung eines Werkzeugs im Menü "Starten". 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 Ausschnitt "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 [Kapitel 4, Workflow des Entwicklers von Überwachungslösungen](#).
- Der Systemadministrator
Informationen hierzu finden Sie unter [Kapitel 5, Workflow des Systemadministrators im Bereich IT-Betrieb](#).

4 Workflow des Entwicklers von Überwachungslösungen



Mike ist ein Entwickler von BSM-Operationenverwaltungs-Überwachungslösungen. Seine wichtigste Aufgabe ist das Anpassen der BSM-Operationenverwaltung an spezielle Geschäftsanforderungen.

In der Regel integriert Mike neue Applikationen und CIs in den Überwachungsprozess. 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:

- Welche KPIs sollten im Überwachungsprozess gemessen werden?
- Wie sollten sie zurück an die Eigner von Geschäftsservices gemeldet werden, die den FTP-Server nutzen?
- 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

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. Zum Beispiel könnte er sich 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-Operationenverwaltung-Werkzeugen für den Neustart des FTP-Servers.
- 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 für die Zuordnung von bestimmten identifizierten Datenträgerproblemen zu bestimmten Problemen mit dem FTP-Server.

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.

Einblicke in diese anderen Rollen erhalten Sie unter:

- Der Systemadministrator
Informationen hierzu finden Sie unter [Kapitel 5, Workflow des Systemadministrators im Bereich IT-Betrieb](#).
- Der Operator
Informationen hierzu finden Sie unter [Kapitel 3, Workflow des Operators](#).

5 Workflow des Systemadministrators im Bereich IT-Betrieb



In [Kapitel 2, Einführung in die BSM-Operationenverwaltung](#), haben wir das Konzept einer Operations Bridge kennen gelernt. Die BSM-Operationenverwaltung ist die Operations Bridge für eine vollständige BSM-Überwachungslösung als zentrale Stelle für das Ereignis- und Leistungsmanagement. Die Operations Bridge ermöglicht das konsolidierte Betriebsmanagement für die BSM-Umgebung.

In [Kapitel 3, 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 Matthew als Systemadministrator im Bereich IT-Betrieb.

Dies ist die letzte Rolle, die wir in unserem Szenario untersuchen möchten. Matthew wirkt im Hintergrund und gestaltet von dort aus eine effiziente Überwachungs Umgebung 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 besitzt das umfassende Fachwissen für die Installation und Konfiguration der BSM-Operationenverwaltung. In einem einfachen Szenario wäre nur eine Instanz der BSM-Operationenverwaltung vorhanden. In einem komplexen Szenario könnten mehrere Instanzen der BSM-Operationenverwaltung in einer verteilten MoM-Umgebung (Manager of Managers) vorhanden sein (siehe [Manager-of-Managers](#) auf Seite 24). In einer MoM-Umgebung erfordert die nahtlose Integration zwischen diesen Umgebungen, dass Matthew HP Operations Orchestration-Workflows, HP Network Node Manager i-Vorfälle (NNMi-Vorfälle) und Business Process Monitor-Ereignisse integrieren muss.

Matthew installiert auch den HP BSM Integration Adapter als Unterstützung bei der Integration von Domänen-Managern von Drittanbietern, wie zum Beispiel Microsoft System Center Operations Manager (SCOM).

Matthew hat die folgenden Verantwortlichkeiten:

- Die BSM-Installation überwachen
- Die Umgebung optimieren
- Infrastruktureinstellungen optimieren
- Benutzer und Benutzerrollen konfigurieren

Die BSM-Installation überwachen

Matthew hat das Fachwissen und Erfahrung mit dem Betriebsmanagement (Operationenverwaltung). Er weiß genau, wie die BSM-Komponenten, einschließlich die 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 weitere HP-Unternehmenslösungen und Applikationen von Drittanbietern, wie zum Beispiel Microsoft SCOM.

Die Komplexität entsteht aus der 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.

Die Umgebung optimieren

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.

Infrastruktureinstellungen optimieren

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.

Benutzer und Benutzerrollen konfigurieren

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. Matthew stellt dem Operator Dave eine Umgebung bereit, die dessen tägliche Aufgaben vereinfacht und sicherstellt, dass dieser 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 Matthew dann installieren muss. Während das Unternehmen wächst, muss Matthew neue Benutzer hinzufügen und jedem von ihnen die geeignete Benutzerrolle und die geeigneten Berechtigungen zuweisen.

Matthew 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 Matthew, 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 Matthew 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 Matthew 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 [Kapitel 4, Workflow des Entwicklers von Überwachungslösungen](#).

- Der Operator

Informationen hierzu finden Sie unter [Kapitel 3, Workflow des Operators](#).

Übersicht

Nachdem Sie etwas über die unterschiedlichen Benutzer, die die täglichen Prozesse von der BSM-Operationenverwaltung installieren, konfigurieren und verwalten, gelesen haben, können Sie erkennen, dass Kompetenzen auf mehreren Gebieten erforderlich sind, damit alles auf einem optimalen Niveau abläuft. 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.