



HP Operations Manager i

Softwareversion: 10.00

OMi-Konzepthandbuch

Dokument-Releasedatum: Januar 2015
Software-Releasedatum: Januar 2015

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 2015 Hewlett-Packard Development Company, L.P.

Marken

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

AMD und das AMD-Pfeilsymbol sind Marken von Advanced Micro Devices, Inc.

Citrix® und XenDesktop® sind eingetragene Marken der Citrix Systems, Inc. und/oder der zugehörigen Tochtergesellschaften. Sie können beim US-Patentamt und Markenämtern in anderen Ländern registriert sein.

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

Intel®, Itanium®, Pentium®, Intel® Xeon® und Lync® sind Marken der Intel Corporation in den USA und anderen Ländern.

Linux® ist eine eingetragene Marke von Linus Torvalds in den USA und anderen Ländern.

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

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

Oracle ist eine eingetragene Marke der Oracle Corporation und/oder ihren Tochterunternehmen.

Red Hat® ist in den USA und anderen Ländern eine eingetragene Marke Red Hat, Inc.

UNIX® ist eine eingetragene Marke von The Open Group.

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:
<https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=>

Auf dieser Website ist ein HP Passport-Konto erforderlich. Wenn Sie nicht über ein Konto verfügen, klicken Sie auf der Seite **HP Passport Sign in** auf die Schaltfläche **Create an account**.

Unterstützung

Besuchen Sie die HP-Website zur Software-Unterstützung unter: <https://softwaresupport.hp.com>

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

Der HP Software Support 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 <https://softwaresupport.hp.com> und klicken Sie auf **Register**.

Weitere Informationen über die für den Zugriff erforderlichen Voraussetzungen erhalten Sie unter: <https://softwaresupport.hp.com/web/softwaresupport/access-levels>

HP Software-Lösungen und -Integrationen sowie bewährte Vorgehensweisen

Besuchen Sie die Website **HP Software Solutions Now** unter <https://h20230.www2.hp.com/sc/solutions/index.jsp> und erfahren Sie, wie die Produkte im HP Software-Katalog zusammenarbeiten, Informationen austauschen und geschäftliche Anforderungen erfüllen.

Besuchen Sie die Website **Cross Portfolio Best Practices Library** unter <https://hpln.hp.com/group/best-practices-hpsw> und greifen Sie auf umfassende Dokumente und Materialien zu bewährten Vorgehensweisen zu.

Inhalt

Kapitel 1: Willkommen zu diesem Handbuch	7
Wie dieses Handbuch aufgebaut ist	7
Wer dieses Handbuch lesen sollte	8
Kapitel 2: Einführung zu Operations Manager i	9
Operations Bridge für eine BSM-Lösung	9
Konsolidiertes Ereignis- und Leistungsmanagement	11
Korrelieren von Ereignissen	14
Topologiebasierte Ereigniskorrelation	16
Strukturierte Problemlösung	18
Management Packs	19
Skalierbare Architektur mit mehreren Servern	21
Monitoring Automation	24
Benutzerengagement	27
Integrationschnittstellen	28
Benutzerrollen und Verantwortlichkeiten	29
Kapitel 3: Workflow des Operators	32
Die Umgebung des Operators	33
Sonstige Rollen	36
Kapitel 4: Workflow des Entwicklers von Überwachungslösungen	37
Erstanalyse	38
Zustandsindikatoren definieren	38
Sonstige Aufgaben	39
Sonstige Rollen	39
Kapitel 5: Workflow des Systemadministrators im Bereich IT-Betrieb	40
Aufgaben im Rahmen der Installation und Konfiguration	40
Die OMi-Installation überwachen	41
Optimieren der Infrastruktureinstellungen	41
Konfigurieren von Benutzern und Benutzerrollen	42
Sonstige Verantwortlichkeiten	42
Ständige Aufgaben	42
Operations Bridge	43

Sonstige Rollen	43
Kapitel 6: Workflow der Applikationsspezialistin	44
Aufgaben im Rahmen der Installation und Konfiguration	44
Ständige Aufgaben	45
Sonstige Rollen	45
Übersicht	46
Senden von Feedback zur Dokumentation	47

Kapitel 1: Willkommen zu diesem Handbuch

Dieses Handbuch bietet eine Einführung in Operations Manager i und zeigt, wie Sie mithilfe dieses Produkts die Effizienz Ihrer IT-Services und -Infrastruktur verbessern können.

Wie dieses Handbuch aufgebaut ist

Dieses Handbuch enthält die folgenden Informationen:

- **"Einführung zu Operations Manager i" auf Seite 9:**
Eine allgemeine Übersicht über die wichtigsten Funktionen veranschaulicht, wie Sie Operations Manager i nutzen können, um die Leistung, Verfügbarkeit und Effizienz Ihrer IT-Umgebung zu verbessern.
- **"Workflow des Operators" auf Seite 32:**
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 40:**
Eine Beschreibung, wie die Rolle von Matthew aussieht und wie er die Operations Manager i-Umgebung überwacht und die Betriebsinfrastruktur so konfiguriert, dass alle Applikationen und Server in seinem Kompetenzbereich integriert werden.
- **"Workflow der Applikationsspezialistin" auf Seite 44:**
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

Kapitel 2: Einführung zu Operations Manager i

In diesem Kapitel finden Sie einen allgemeinen Überblick über Operations Manager i 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 Operations Manager i in eine Business Service Management-Lösung (BSM-Lösung) passt, und beschreibt die zugrunde liegenden Konzepte.

Das Kapitel ist wie folgt strukturiert:

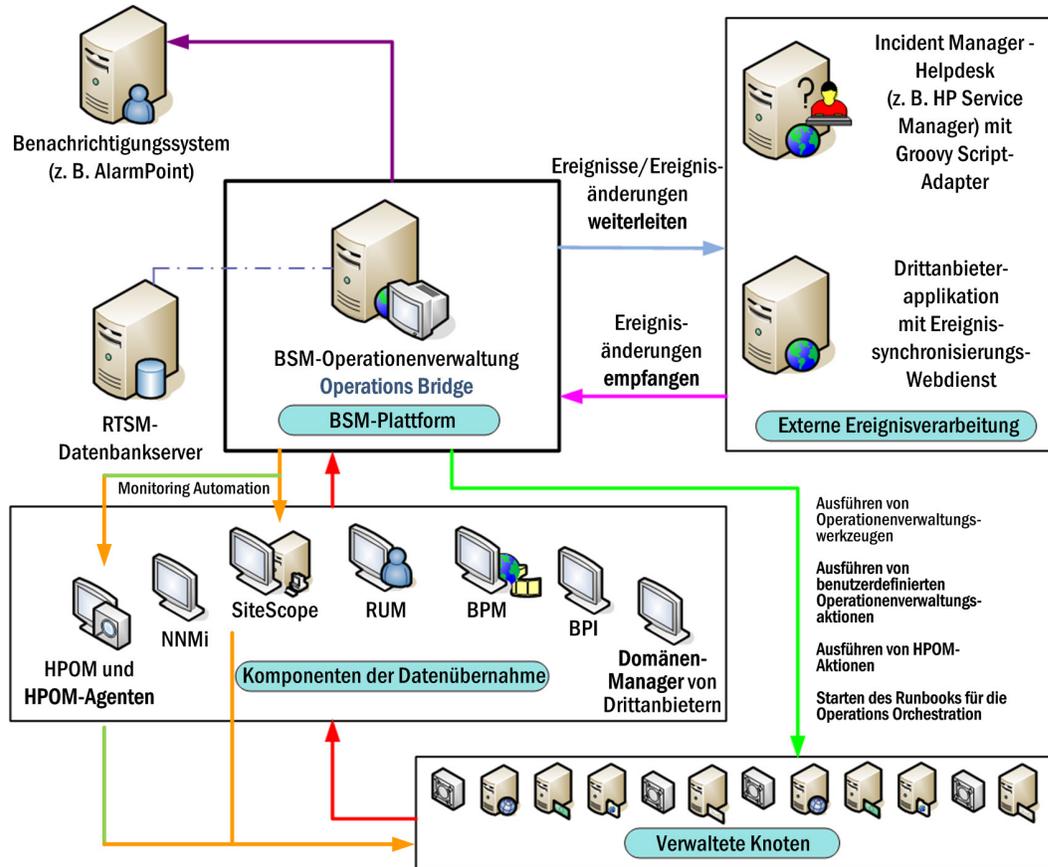
- ["Operations Bridge für eine BSM-Lösung" unten](#)
- ["Konsolidiertes Ereignis- und Leistungsmanagement" auf Seite 11](#)
- ["Strukturierte Problemlösung" auf Seite 18](#)
- ["Management Packs" auf Seite 19](#)
- ["Skalierbare Architektur mit mehreren Servern" auf Seite 21](#)
- ["Monitoring Automation" auf Seite 24](#)
- ["Integrationschnittstellen" auf Seite 28](#)
- ["Benutzerrollen und Verantwortlichkeiten" auf Seite 29](#)

Operations Bridge für eine BSM-Lösung

OMi bildet die Basis für die Ereignisverwaltung für eine vollständige Business Service Management-Überwachungslösung (BSM). 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, das auf Business Service Management und das IT-Infrastrukturmanagement dieselben Prozesse anwendet.

OMi verknüpft das Infrastrukturmanagement mit dem Management von Applikationen und Geschäftsservices. Es kombiniert Ereignisse aus HP Application Management-Komponenten, wie Business Process Monitor (BPM), Real User Monitor (RUM) und Service Level Management (SLM), mit Ereignissen aus System- und Netzwerkprodukten, wie HP Operations Manager (HPOM) und HP Network Node Manager i (NNMi). Dies ermöglicht die Verfolgung aller Ereignisse, die in Ihrer überwachten Umgebung auftreten.

Die folgende Abbildung zeigt ein Beispiel für eine typische Bereitstellung, bei der OMi die Operations Bridge in einer BSM-Lösung ist. OMi ermöglicht die automatisierte Überwachung und Integration von mehreren externen Applikationen.



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. OMi hilft Ihnen, ereignisbezogene Probleme zu finden und zu lösen, bevor sich die Qualität der Geschäfts-services 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

Die Ereignisse werden ungeachtet dessen, woher sie stammen, auf einheitliche Art und Weise verarbeitet und verwaltet.

Beispiele für Ereignisquellen:

- HP Operations Agents, konfiguriert über OMi
- 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)
- HP Business Process Monitor (BPM)
- HP Real User Monitor (RUM)
- HP SiteScope
- HP Systems Insight Manager
- 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 OMi sind auch im [HP Live Network](#) 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 OMi 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 aller 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 nützlichsten Informationen konzentrieren, zum Beispiel um die Ereignisse mit der höchsten Priorität zu finden und festzustellen, welche dieser Ereignisse zuerst bearbeitet werden müssen, um ihre 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 OMi weiterleiten. Ereignisse werden zwischen den Servern synchronisiert. Zum Beispiel synchronisieren OMi und HP Operations Manager (HPOM) den Zustand von Ereignissen und Nachrichten. Wenn ein OMi-Operator ein Ereignis schließt, wird automatisch eine Benachrichtigung an HPOM gesendet. Analog wird OMi von HPOM über die Bestätigung von Nachrichten benachrichtigt und OMi setzt die entsprechenden Ereignisse automatisch auf den neuen Lebenszyklusstatus "geschlossen".

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

Überwachungs-Dashboards

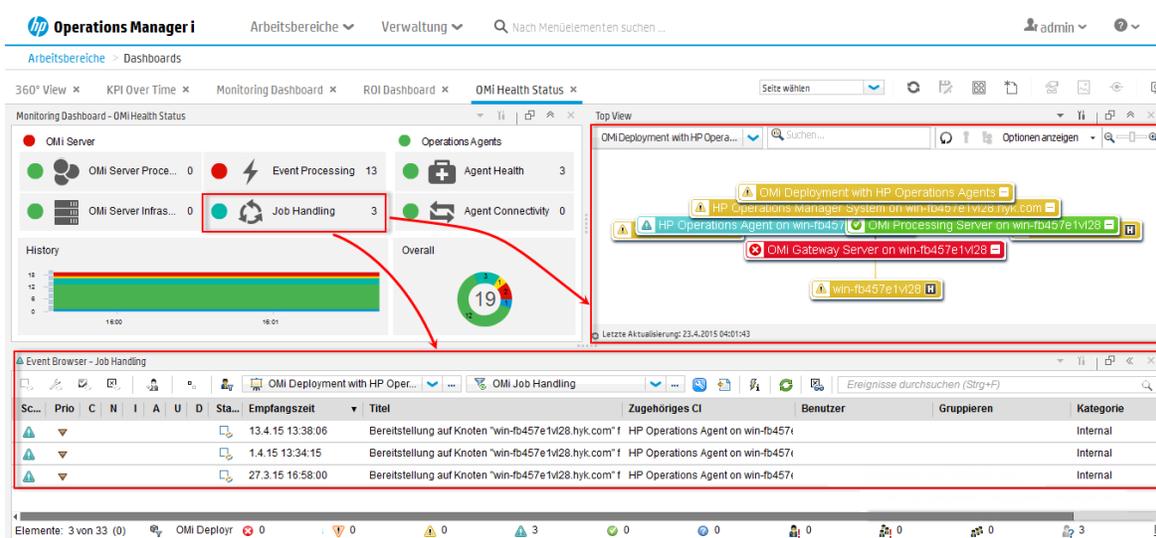
Überwachungs-Dashboards bieten auf einen Blick eine Übersicht der Ereignisse aus Ihrer überwachten Umgebung. Sie ermöglichen Ihnen, den Zustand der Umgebung schnell zu erfassen und Bereiche zu identifizieren, die Ihre Aufmerksamkeit erfordern.

Mit Überwachungs-Dashboards können Sie:

- Sich einen Überblick 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 Überwachungs-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.

Die folgende Abbildung zeigt einen Bildschirm des Überwachungs-Dashboards:

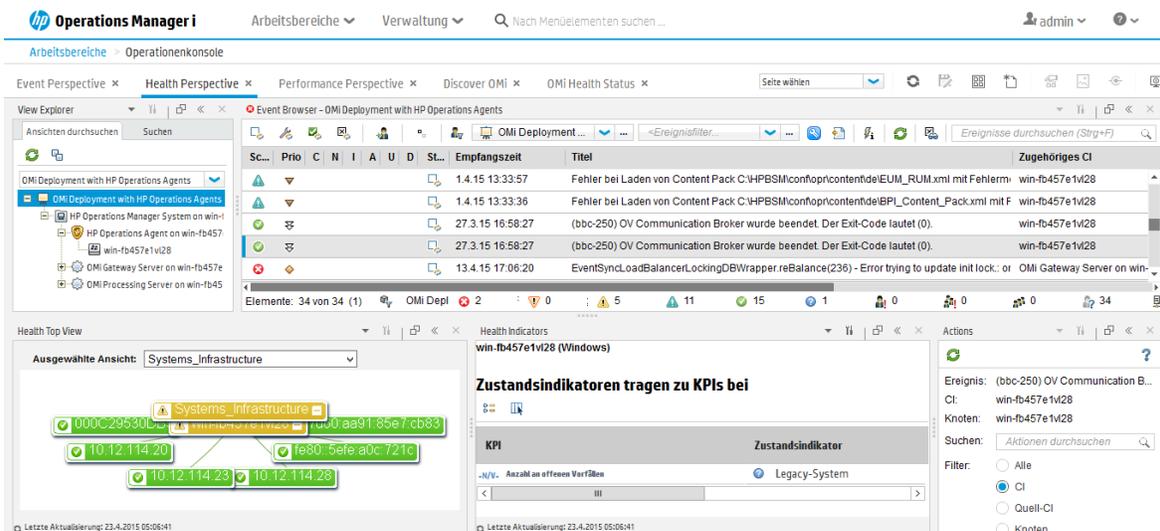


Zustandsinformationen

Mit ereignisbasierten Daten können Sie im Ereignis-Browser sehen, welches zugehörige CI durch das Ereignis betroffen ist. Außerdem werden OMi-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.

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



Sie sehen den Zustand eines Objekts, die zugehörigen KPIs und Zustandsindikatoren und die Auswirkungen des Zustands des ausgewählten Objekts auf den Zustand zugehöriger Objekte. Sie können beispielsweise den Zustand der benachbarten CIs überprüfen. Mit diesen Informationen können Sie analysieren, auf welche Ereignisse Sie sich konzentrieren sollten, 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.

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 OMi 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 LANGSAM" 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 OK" 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, indem automatisch die Ereignisse 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 fehlt, 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 Ursachenergebnis "Server1: CPU dauerhaft überlastet (100 % für mehr als 10 Minuten)" erklärt werden.

Der Schlüssel besteht darin, die zugrunde liegenden Ursachenergebnisse genau zu bestimmen, die für andere Symptomereignisse verantwortlich sind, damit Sie die Auflösung dieser Ursachenergebnisse 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 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 deutlich höhere Last auf den Servern. Um diese Situation zu vermeiden, kann OMi 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 Skripten, einschließlich Beispielskripten, die mit dem Produkt bereitgestellt werden, finden Sie im *Operations Manager i Extensibility Guide*.

- **HP Operations Agent-Aktionen**

Die Ereignisse, die im Ereignis-Browser von HP Operations Agent oder HPOM empfangen werden, können ereignisbezogene Aktionen enthalten, die entsprechend Richtlinienvorlagen in OMi oder in HPOM-Richtlinien konfiguriert sind. Falls es ereignisbezogene Aktionen gibt, können Sie diese Aktionen über die OMi-Konsole ausführen. Diese Aktionen können entweder vom Operator initiiert oder automatisch ausgeführt werden, wenn ein Ereignis eintritt.

- **Starten von Runbooks in HP Operations Orchestration**

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 OMi zugeordnet werden. Sie können OO-Runbooks in einem Ereigniskontext über die OMi-Konsole 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.

- **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. OMi-Grafiken können Metriken aus HP Operations Agent-, HP SiteScope-, HP vPV-, BSM Connector- und Application Management-Systemen anzeigen. 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 OMi 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 Regelaktionen 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 bereitstellen, indem Sie Ereignisse mit Tipps und Hinweisen versehen, die das Verständnis verbessern und das dem Ereignis zugrunde liegende Problem erläutern.

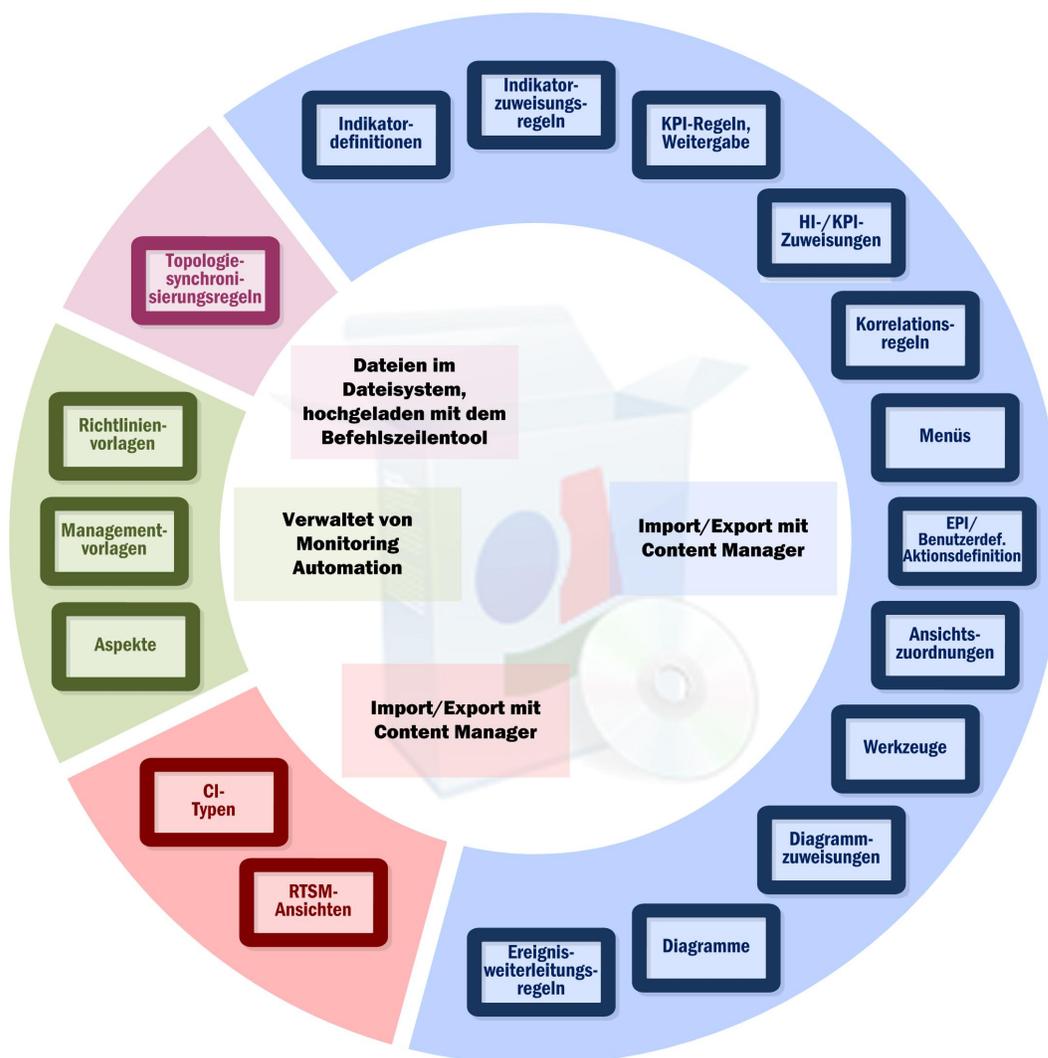
Management Packs

Management Packs enthalten Add-On-Inhalte für OMi. Sie bieten automatische und End-to-End-Überwachungslösungen für Infrastruktur und Applikationen. Management Packs ermöglichen es

Benutzern, Probleme in der IT-Domäne zu überwachen, zu erkennen und zu beheben. Sie erhöhen die Produktivität der Benutzer durch Optimierung und Automatisierung verschiedener Aufgaben und verringern die MTTR (Mean Time To Resolve, durchschnittliche Behebungsdauer) von Vorfällen.

Management Packs ermitteln Applikationsdomänen und überwachen die Domänen proaktiv auf Verfügbarkeits- und Leistungsprobleme. Dazu gehören z. B. Managementvorlagen, Aspekte, Richtlinienvorlagen, Leistungsdiagramme, Werkzeuge für die Fehlerbehebung, automatische Lösungsabläufe, Zustandsindikator- und KPI-Definitionen sowie Regeln für die topologiebasierte Ereigniskorrelation (Topology-Based Event Correlation, TBEC).

In die folgenden Abbildung enthält eine Übersicht über den Inhalt, der sich in einem Satz Management Packs befinden kann.



Vordefinierte Management Packs

Ein von HP bereitgestelltes Management Pack besteht üblicherweise aus einem RTSM-Paket, einem Content Pack, Handbüchern und der Onlinehilfe. Alle diese Inhalte werden automatisch während der Management Pack-Installation hochgeladen. Zur Verwendung eines Management Packs kann eine separate Lizenz erforderlich sein.

Werkzeuge zur Verwaltung von Inhalten

OMi enthält einen Satz mit Werkzeugen, um Sie bei der Verwaltung eigener Inhalte zu unterstützen. Diese Werkzeuge sind der RTSM Package Manager und der Content Packs Manager. Mit diesen Werkzeugen können Sie eigene Inhalte packen und die Inhalte 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 Export- und Importwerkzeugen können Sie Inhalte zwischen Systemen austauschen, sodass 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 Operations Manager i 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 OMi-Instanzen 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 OMi 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 OMi-Servern und Domänen-Managern von Drittanbietern zusammenarbeiten.

In einer solchen hierarchischen, verteilten Umgebung können Sie OMi für die folgenden Zwecke konfigurieren:

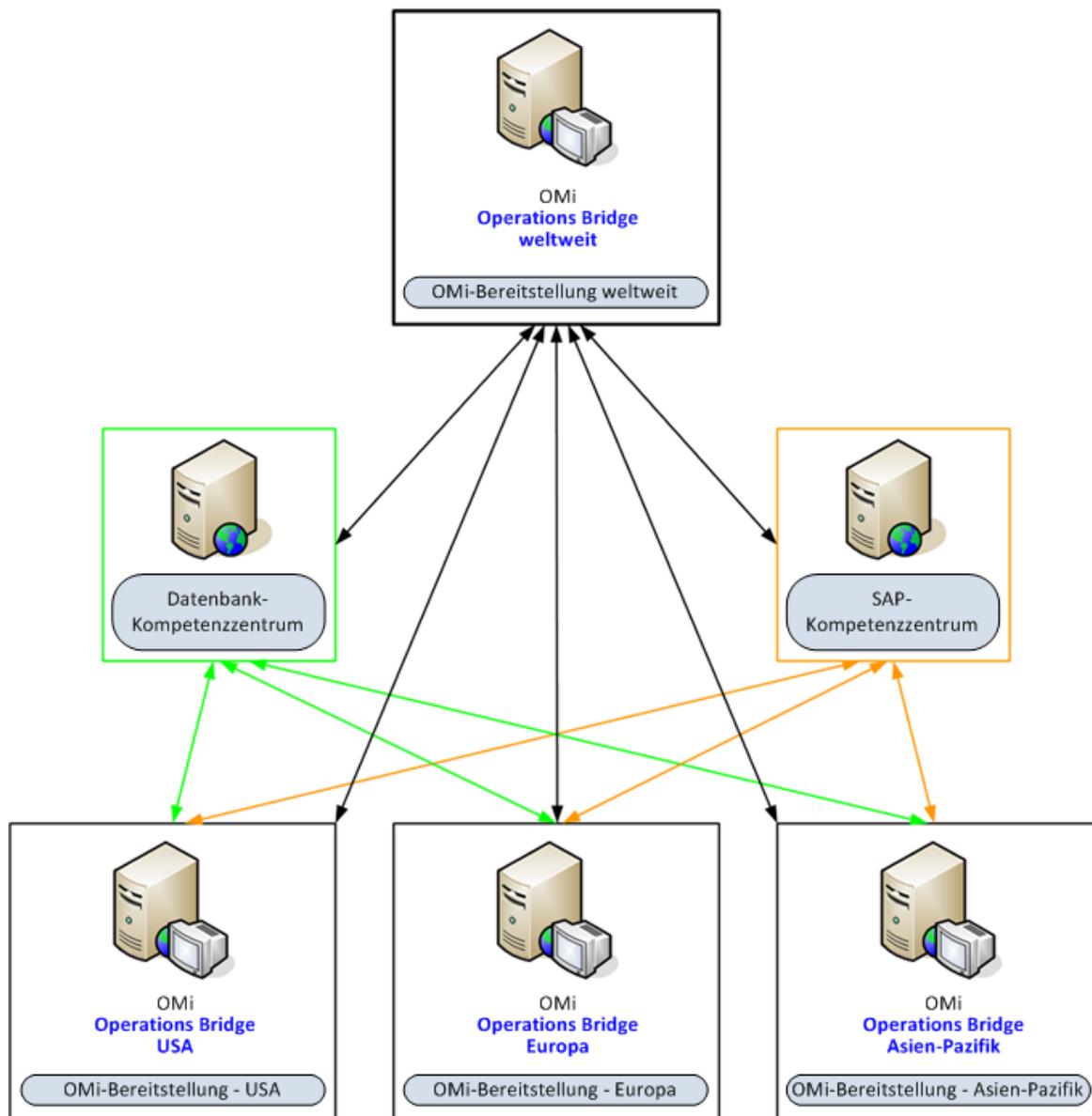
- Für die Funktion als "Manager of Managers" (MoM), also für die zentrale Ereigniskonsolidierung der gesamten Umgebung an der Spitze der Hierarchie.
- Für die Zusammenarbeit mit anderen HP-Produkten, wie zum Beispiel NNMi und HP SiteScope.
- Für die Zusammenarbeit mit Domänen-Managern von Drittanbietern,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

Sie können Server, auf denen OMi betrieben wird, für die folgenden Zwecke konfigurieren:

- Für die Weiterleitung von Ereignissen an andere Server, auf denen OMi 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 OMi und HPOM-Management-Server betrieben werden.
- Für den Empfang von Ereignissen, die von einem BSM 9.x-Server weitergeleitet werden, der von APM-Applikationen, wie zum Beispiel HP Business Process Monitor (BPM), Warnungen empfängt.

Manager-of-Managers

Die folgende Abbildung zeigt ein Beispiel für eine hierarchische, verteilte Umgebung mit einem zentralen Server, auf dem OMi betrieben wird und der nach dem Prinzip des serverbasierten flexiblen Managements andere regionale Server, auf denen OMi betrieben wird, verwaltet.



In diesem Beispiel verwalten Implementierungen auf den regionalen Servern OMi Europe, OMi USA und OMi Asia Pacific unterschiedliche Regionen. OMi in der Implementierung auf dem Server OMi Worldwide befindet sich an der Spitze der Hierarchie und verwaltet die regionalen Server. Dies ist der MoM, also die zentrale Ereigniskonsolidierung für die gesamte Umgebung. Es handelt sich um eine weltweite Operations Bridge. Die regionalen Server können in ihren Regionen auch als Manager 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.

Im Beispielszenario leiten alle regionalen Server (OMi Europe, OMi USA und OMi 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.

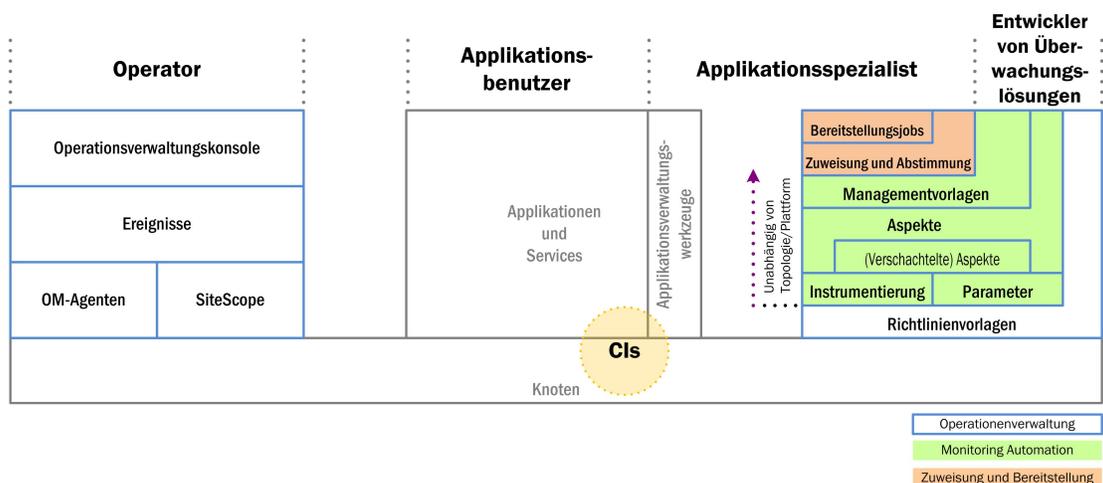
Monitoring Automation

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 der folgenden Abbildung dargestellten Stapel an.



Die Basis des Stapels steht für die Clis, die überwacht werden sollen. Clis können Netzwerkelemente wie Computer aber auch Applikationen oder Gruppen von Applikationen sein, die einen Service bereitstellen. Der Zugriff auf Clis erfolgt auf folgende Weise:

- Benutzer interagiert mit den Clis unabhängig von jeder Überwachung, wie im zentralen Abschnitt der Abbildung angedeutet wird.
- OMi überwacht die Clis mithilfe der vertrauten Überwachungsstruktur, wie im linken Abschnitt der Abbildung gezeigt wird.
- Ein Entwickler konfiguriert Überwachungslösungen, wie im rechten Abschnitt der Abbildung 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.

Monitoring Automation bietet eine Reihe von Funktionen für die Erstellung von flexiblen Überwachungslösungen. Im folgenden Abschnitt werden die einzelnen Konfigurationselemente der Reihe nach erläutert. 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. Clis sind der eigentliche Gegenstand der Überwachung durch OMi. Ereignisse beziehen sich immer auf Clis.

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 Aspekzebene 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 OMi mitteilt, 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 Aspekzebene 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. Um mit der Überwachung zu beginnen, 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 OMi 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.

Benutzerengagement

Die innovative Funktion **Benutzerengagement** setzt Spielmechanismen ein, um einen zusätzlichen Anreiz für OMi-Benutzer zu bieten. Den Benutzern werden Aufgaben zur Prozessoptimierung gestellt, um auf diese Weise die Prozesseffizienz zu erhöhen und das Know-how der Benutzer zu erweitern. Das erfolgreiche Absolvieren der verschiedenen Stufen wird mit Auszeichnungen und Echtzeit-Benachrichtigungen über die herausragende Leistung belohnt, um die intensivere Beschäftigung mit OMi 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 "Benutzerengagement" zu einem leistungsfähigen Feature macht.

Durch das Festlegen geschäftsorientierter Auszeichnungen, auf die OMi-Benutzer 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.

"Benutzerengagement" nutzt intrinsische Beweggründe, um die OMi-Benutzer 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. "Benutzerengagement" bietet ein Gerüst, mit dem Sie den Benutzern helfen können, die Verwendung von OMi 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 "Benutzerengagement" können integrierte Auszeichnungen auswählen, konfigurieren und aktivieren, die an die Bedürfnisse der verschiedenen OMi-Benutzer 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.

Integrationschnittstellen

Die bereitgestellten Schnittstellen ermöglichen die Verknüpfung 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 Ereignisverarbeitungsipeline 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 Links zu externen Wissensdatenbanken.

- 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 OMi und einer externen Ereignisverarbeitungsapplikation stellt OMi eine Webserviceschnittstelle für die Ereignissynchronisierung bereit. Ein typischer Anwendungsfall ist die Synchronisierung von Ereignissen zwischen OMi und einem Vorfalls-Manager, wie zum Beispiel Service Manager.
- Zur direkten Verknüpfung mit anderen Domänen-Managern, wie zum Beispiel Microsoft Systems Center Operations Manager, stellt OMi den HP BSM Connector bereit.

Im OMi Extensibility Guide in der OMi-Dokumentationsbibliothek finden Sie die Beschreibung dieser Schnittstellen sowie Informationen für die Entwickler von Inhalten und die Integrationsverantwortlichen zur Anpassung und Erweiterung der Funktionalität von OMi.

Benutzerrollen und Verantwortlichkeiten

Für das Installieren, Konfigurieren und Ausführen der Operations Bridge ist ein Team aus Personen mit speziellen Kompetenzen 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 neue Benutzer im OMi-Bereich 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 Überwachereignisse auf ein Problem hinweisen.

In der Tabelle unten finden Sie häufig verwendete Titel für diese Benutzerrollen sowie eine Übersicht über ihre Verantwortlichkeiten. Nachdem wir mehr über OMi wissen, begleiten wir in den folgenden Kapiteln einige typische Benutzer, 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 OMi als Operations Bridge fungiert.

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 OMi-fremde Routineoperationen für die Applikationen, Systeme und Netzwerke aus, für die er verantwortlich ist.</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 	<ul style="list-style-type: none"> • Passt die Art und Weise an, in der OMi eine Domäne überwacht. • Konfiguriert Managementvorlagen, Aspekte und Richtlinienvorlagen für Monitoring Automation.
<p>Administrator</p>  <p>"Matthew"</p>	<ul style="list-style-type: none"> • Systemadministrator • Systemadministrator im Bereich IT-Betrieb • OMi-Administrator • Systemarchitekt 	<p>Überwacht die OMi-Umgebung und Aufgabenzuweisungen.</p> <p>Verknüpft OMi mit anderen Werkzeugen und Prozessen.</p>
<p>Applikationsspezialistin</p>  <p>"Alice"</p>	<ul style="list-style-type: none"> • Expertin für eine bestimmte Applikation oder einen bestimmten Service • Applikationsadministrator 	<p>Optimiert eine Überwachungslösung für die jeweilige Applikations- oder Serviceumgebung und weist Managementvorlagen oder Aspekte zu Systemknoten zu.</p> <p>Implementiert die Überwachungslösung und stellt sicher, dass die Überwachung ordnungsgemäß ausgeführt wird.</p>

Kapitel 3: Workflow des Operators



Im Kapitel "Einführung zu Operations Manager i" haben wir Dave kennengelernt. Dave ist der Operator, der für das tägliche Management in einer OMi-Bereitstellung verantwortlich ist. Ein Operator ist in der IT-Umgebung eines Unternehmens in der Regel eine Stelle auf Einstiegsebene, aber Dave bringt bereits diverse Fähigkeiten mit, da er bereits Erfahrung mit vielen der Technologien in der Operations Manager i-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 Operations Manager i-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.

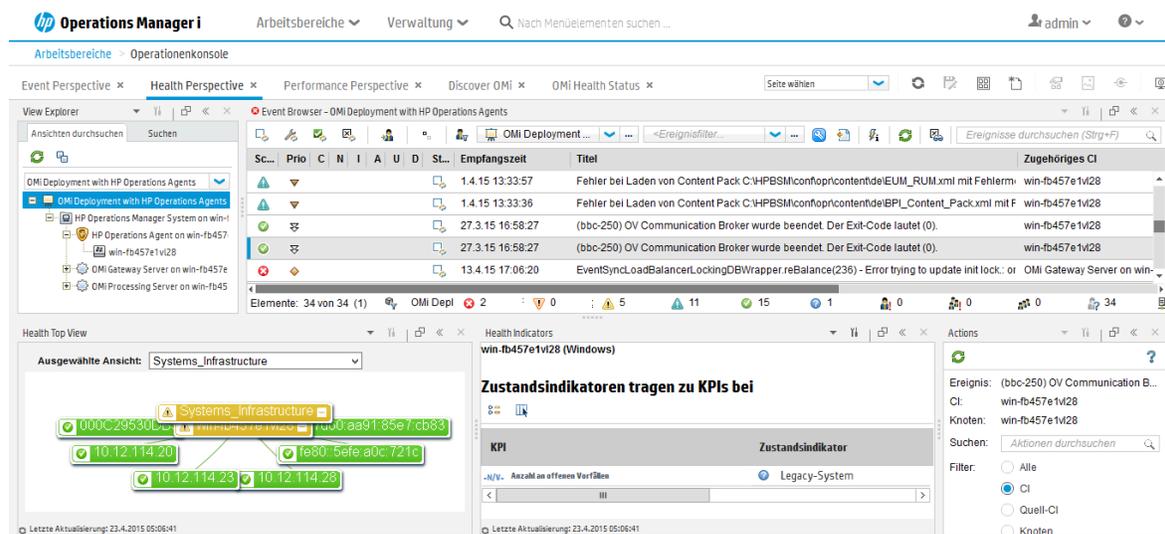
Wenn Dave ein Problem nicht beheben kann, kann er es eskalieren, indem er das Ereignis an eine externe Ereignisverarbeitungsapplikation weiterleitet. Dies umfasst in der Regel auch die Übertragung des Ereignisbesitzes, beispielsweise an einen Helpdesk-Operator oder einen Applikationsspezialisten.

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

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

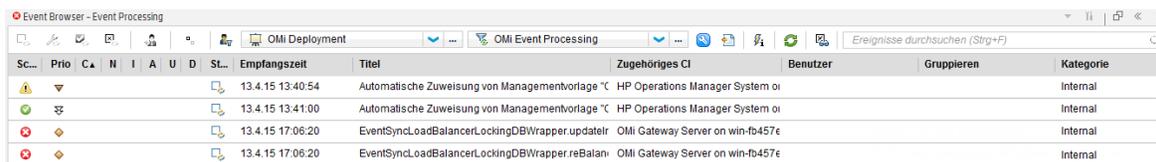
- Der Ausschnitt **Zustandsindikatoren** enthält detaillierte Informationen zum Status des CI, das im Ausschnitt **Zustandstopologieansicht** ausgewählt wurde. Diese Ansicht enthält Informationen zu den Leistungs-KPIs, Verfügbarkeits-KPIs und allen Zustandsindikatoren, die für das ausgewählte CI relevant 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.

Die folgende Abbildung zeigt eine typische globale Ansicht mit Ereignisinformationen im Ausschnitt **Ereignis-Browser**.

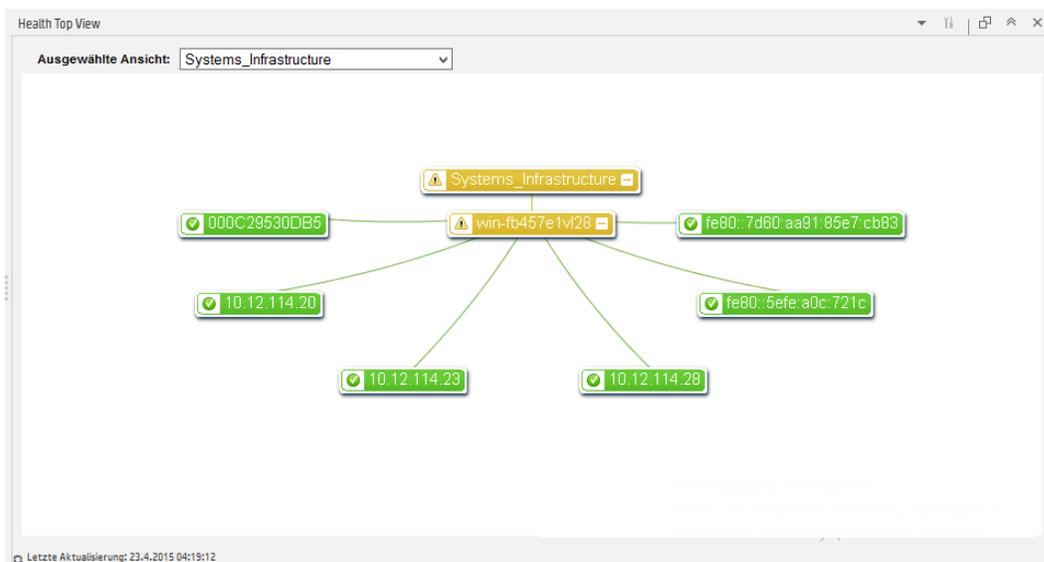


Sc...	Prio	Ca	N	I	A	U	D	St...	Empfangszeit	Titel	Zugehöriges CI	Benutzer	Gruppieren	Kategorie
!									13.4.15 13:40:54	Automatische Zuweisung von Managementvorlage	HP Operations Manager System or			Internal
!									13.4.15 13:41:00	Automatische Zuweisung von Managementvorlage	HP Operations Manager System or			Internal
!									13.4.15 17:06:20	EventSynclBalancerLockingDBWrapper.update	OMI Gateway Server on win-fb457e			Internal
!									13.4.15 17:06:20	EventSynclBalancerLockingDBWrapper.reBalanc	OMI Gateway Server on win-fb457e			Internal

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. Die folgende Abbildung zeigt eine typische Zustandstopologieansicht von Geschäftsservices und CIs.



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.

KPI	Zustandsindikator	Status	Wert	Letzte Statusän
-N/A- Anzahl an offenen Vorfällen	Legacy-System	Unbekannt	N/A	-

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: Operations Manager i-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 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 37](#).
- Der Systemadministrator
Informationen hierzu finden Sie unter "[Workflow des Systemadministrators im Bereich IT-Betrieb](#)" auf [Seite 40](#).

Kapitel 4: Workflow des Entwicklers von Überwachungslösungen



Mike ist ein Entwickler von OMI-Überwachungslösungen. Seine wichtigste Aufgabe ist das Anpassen von OMI 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 and 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 OMi-Werkzeugen für den Neustart des FTP-Servers.
- Erstellen von mehreren operativen Runbooks. Mike könnte beispielsweise 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. 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 40](#).
- Der Operator
Informationen hierzu finden Sie unter ["Workflow des Operators" auf Seite 32](#).
- Die Applikationsspezialistin
Informationen hierzu finden Sie unter ["Workflow der Applikationsspezialistin" auf Seite 44](#).

Kapitel 5: Workflow des Systemadministrators im Bereich IT-Betrieb



In Kapitel "Einführung zu Operations Manager i" haben wir das Konzept einer Operations Bridge kennen gelernt. OMi ist die Operations Bridge für eine vollständige Business Service Management-Lösung und stellt einen zentralen Ort für das Ereignis- und Leistungsmanagement bereit.

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 OMi zu installieren, zu konfigurieren und mit anderen Applikationen wie HP Operations Orchestration oder HP Service Manager zu verknüpfen. Darüber hinaus konfiguriert er die Ereignisweiterleitung von verschiedenen Quellen wie HP Network Node Manager i- (NNMi) oder HPOM-Systemen.

Außerdem aktiviert Matthew den Überwachungsprozess durch die Installation der erforderlichen Überwachungswerkzeuge wie Operation Agents und HP SiteScope.

Matthew ist zudem für die Installation und Pflege von Management Packs oder benutzerdefinierten Content Packs zuständig.

Falls erforderlich, installiert Matthew auch HP BSM Connector, um die Integration von Domänen-Managern von Drittanbietern, beispielsweise Microsoft System Center Operations Manager, zu unterstützen.

Matthew hat die folgenden Verantwortlichkeiten:

- Die OMi-Installation überwachen
- Optimieren der Umgebung
- Optimieren der Infrastruktureinstellungen
- Konfigurieren von Benutzern und Benutzerrollen

Die OMi-Installation überwachen

Matthew verfügt über Fachwissen und Erfahrung mit OMi. Er weiß, wie OMi installiert und ordnungsgemäß konfiguriert werden muss. Er entwirft und beaufsichtigt den kompletten Prozess zur Installation der erforderlichen OMi-Komponenten und entscheidet, welche Applikationen in OMi 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 OMi 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
- Definieren von Arbeitsbereichsseiten und Überwachungs-Dashboards für verschiedene Benutzer

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. Bei Bedarf muss Mike möglicherweise auch Patches für Operations Agents bereitstellen.

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 von OMi 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 37](#).
- Der Operator
Informationen hierzu finden Sie unter ["Workflow des Operators"](#) auf [Seite 32](#).

Kapitel 6: Workflow der Applikationsspezialistin



In Kapitel "[Einführung zu Operations Manager i](#)" haben wir das Konzept einer Operations Bridge kennen gelernt. OMi ist die Operations Bridge für eine vollständige Business Service Management-Lösung und stellt einen zentralen Ort für das Ereignis- und Leistungsmanagement bereit.

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. Sie entscheidet, ob Werte in der Managementvorlage oder der automatischen Zuweisungsregel geändert werden müssen oder ob sie Werte für bestimmte CIs, die die konkrete Applikationsinstanz repräsentieren, manuell überschreiben wird.

- OMi 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 OMi 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 OMi die Aspekte in der Managementvorlage bereit.

Ständige Aufgaben

Es ist möglich, dass ein Operator, beispielsweise Dave, Kontakt zu Alice aufnimmt, falls mehrere Ereignisse generiert werden, obwohl kein echtes Problem aufgetreten ist. Dies kann passieren, wenn Schwellenwerte fälschlicherweise zu niedrig eingestellt wurden. In diesem Fall muss Alice die Überwachungskonfiguration optimieren und die Schwellenwertparameter für bestimmte CIs, in automatischen Zuweisungsregeln oder in Managementvorlagen ändern.

Sonstige Rollen

Alice, die Applikationsspezialistin, 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 37](#).
- Der Operator
Informationen hierzu finden Sie unter "[Workflow des Operators](#)" auf [Seite 32](#).

Übersicht

Nachdem Sie etwas über die unterschiedlichen Benutzer erfahren haben, die Operations Manager i installieren, konfigurieren und für den täglichen Betrieb zuständig sind, ist deutlich geworden, dass Fähigkeiten in mehreren Gebieten erforderlich sind, damit alles optimal abläuft. Möglicherweise haben auch Sie eine der Funktionen, die in diesem Handbuch beschrieben werden. Unabhängig von der Rolle, die Sie übernehmen, können Sie Ihren Beitrag dazu leisten, wie gut Ihre Arbeitsgruppe Ihren internen Kunden einen Nutzen bereitstellt.

Senden von Feedback zur Dokumentation

Wenn Sie Anmerkungen zu diesem Dokument haben, können Sie sich per E-Mail [an das Dokumentationsteam wenden](#). Ist auf Ihrem System ein E-Mail-Client installiert, klicken Sie auf den Link oben und ein E-Mail-Fenster mit folgendem Betreff wird geöffnet:

Feedback zu OMi-Konzepthandbuch (Operations Manager i 10.00)

Geben Sie Ihr Feedback ein und klicken Sie auf **Senden**.

Falls kein E-Mail-Client verfügbar ist, kopieren Sie Ihren Text in einem Webmail-Client in eine neue Nachricht und senden Sie diese an ovdoc-asm@hp.com.

Ihr Feedback ist uns willkommen!



[Gehe zu OMi!](#)