IBM Intelligent Operations Center

IBM Intelligent Operations Center Produktdokumentation

Version 1 Release 5

IBM Intelligent Operations Center

IBM Intelligent Operations Center Produktdokumentation

Version 1 Release 5

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 381 gelesen werden.

Diese Ausgabe bezieht sich auf IBM Intelligent Operations Center Version 1, Release 5, Modifikation 0. Sie gilt für alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Intelligent Operations Center, Product Documentation, Version 1 Release 5,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
TSC Germany
Kst. 2877
Mai 2013

Inhaltsverzeichnis

Kapitel 1. Übersicht über die Lösung

In vielen Unternehmen und Projekten spielt die effiziente operative Überwachung und Koordination eine wichtige Rolle. Sie weisen alle die Gemeinsamkeit auf, dass die richtigen Informationen zusammengeführt werden müssen. Nur so wird ermöglicht, dass die richtigen Personen schnelle, korrekte Entscheidungen treffen und die Auswirkung dieser Entscheidungen verfolgen können. Die Softwarelösung IBM® Intelligent Operations Center wurde entwickelt, um die effektive Überwachung und Koordination von Operationen zu vereinfachen.

Behörden müssen sich häufig mit denselben Problemen bezüglich ihrer Kernsysteme auseinandersetzen und stehen vor der Aufgabe, ihre vernetzten Systeme verbessern zu müssen. Zukunftsorientierte Behörden möchten von der höheren Effizienz und Effektivität profitieren, die durch intelligentere Kernsysteme ermöglicht wird. Dabei beschreiten sie neue Wege bei der Ausschöpfung des Potenzials dieser Systeme. Durch den Einsatz fortgeschrittener Informationstechnologie können Verhaltens- und Ereignismuster von den Behörden schneller erkannt und vorhergesagt werden. Auf diese Weise haben sie die Möglichkeit, auf intelligente Weise darauf zu reagieren.

IBM legt als Maßstab für eine intelligente Stadt beispielsweise die Verbesserung der Lebensqualität und der wirtschaftlichen Lage an, die durch den Einsatz von Informationstechnologie (IT) erzielt werden kann, wenn diese für die Planung, das Design, den Aufbau und den Betrieb der städtischen Infrastruktur genutzt wird. Eine intelligente Stadt dreht sich also nicht in erster Linie um "die neueste Technologie". Vielmehr sollen innovative Mittel und Wege gefunden werden, die bereits vorhandenen Ressourcen mithilfe der Technologie bestmöglich zu nutzen. Dabei steht stets die Verbesserung der Lebensqualität der Einwohner einer Stadt im Vordergrund.

Das IBM Intelligent Operations Center nutzt das Potenzial der von Computersystemen generierten Echtdaten wie folgt:

- Die richtigen Daten werden erfasst und verwaltet
- Diese Daten werden integriert und analysiert
- Ein einfacher und rechtzeitiger Informationszugriff wird ermöglicht
- Zugehörige Informationen werden kohärent dargestellt

Diese Lösung bietet folgende Vorteile:

- Durch die Anpassung von Systemen werden Ergebnisse auf Basis der gewonnenen Erkenntnisse geliefert
- Optimierung geplanter und ungeplanter Operationen mithilfe eines ganzheitlichen Ansatzes zur Berichterstellung und Überwachung
- Aufbau einer Konvergenz zwischen den Domänen in einem Unternehmen durch die Vereinfachung der Kommunikation und Zusammenarbeit
- Verbesserung der Servicequalität und Reduzierung der Kosten durch die Koordination von Ereignissen

Eine Operation kann in einzelne Domänen unterteilt werden, die sich für gewöhnlich an der Organisationsstruktur und am Sachgebiet der beteiligten Personen orientieren. In einer Stadt gibt es für die einzelnen Sachgebiete eigene Abteilungen, die sich beispielsweise mit dem Transportwesen, der Wasserversorgung und der öffentlichen Sicherheit befassen.

Mit der steigenden Komplexität der Operationen in einer Domäne wird auch eine angepasstere Lösung erforderlich. Das IBM Intelligent Operations Center bietet verschiedene Integrationspunkte, an denen eine Anpassung vorgenommen werden kann. Durch diese Integrationspunkte und die enthaltene Infrastruktur können IBM Business Partner, Service-Provider und Kunden eine breitgefächerte und leistungsstarke Lösung flexibel gestalten.

Zielgruppe

Dieses Information Center richtet sich an Personen, die das IBM Intelligent Operations Center verwenden, installieren, verwalten und pflegen. Es enthält unter anderem auch eine Dokumentation der Implementierung zur Anpassung der Lösung und Integration der externen zugrunde liegenden Systeme, die vom IBM Intelligent Operations Center benötigt werden.

Bei diesem Information Center wird vorausgesetzt, dass die Benutzer die im Lieferumfang dieser Lösung enthaltenen Produkte bereits kennen und mit ihren Funktionen vertraut sind. Bei diesem Information Center wird ebenfalls vorausgesetzt, dass die Benutzer über Grundkenntnisse des Red Hat Enterprise Linux-Betriebssystems verfügen. Schulungen für die im Lieferumfang enthaltenen Produkte oder das Betriebssystem liegen nicht in der Zuständigkeit dieses Information Centers. Falls Sie eine Schulung für diese Produkte benötigen, bitten Sie Ihren Systemintegrator oder IBM Ansprechpartner um Informationen zu Schulungsmöglichkeiten für die Basiskomponenten.

Links zur Produktdokumentation der Komponente finden Sie im Referenzabschnitt am Ende des Themas.

Zugehörige Konzepte:

„Zusätzliche Produktinformationen" auf Seite 378
Die folgenden zusätzlichen Informationen stehen online zur Verfügung.

Funktionen

Das IBM Intelligent Operations Center bietet Funktionen zur Messung, Überwachung und Modellierung, die zugrunde liegende Systeme in eine Einzellösung integrieren und somit die Geschäftsabläufe effizienter gestalten sowie die Planung und Koordination verbessern sollen.

Das IBM Intelligent Operations Center ist eine Lösung der Produktfamilie IBM Smarter Cities Software Solutions. Das IBM Intelligent Operations Center kann (vor Ort) auf der bereits vorhandenen Hardware installiert oder in der Cloud implementiert werden. Das IBM Intelligent Operations Center kann einzeln oder gemeinsam mit anderen Lösungen aus der Produktfamilie IBM Smarter Cities Software Solutions installiert werden.

Das IBM Intelligent Operations Center ist eine grafisch orientierte Lösung mit rollenbasiertem Zugriff auf Ereignisse für ein Unternehmen und die zugrunde liegenden Domänen. Es verfügt über Ereignismanagementfunktionen, über integrierte Zuordnungsfunktionen sowie über Funktionen für die Ressourcenüberwachung. Die Lösung kann die entsprechenden Verfahren und Workflows für Aktivitäten als Vorbereitung für und Reaktion auf Ereignisse bereitstellen und protokollieren. Darüber hinaus bietet sie für eine höhere Effektivität eine KPIs-basierte Berichterstellung und Funktionen für die Onlinezusammenarbeit. Diese Funktionen ermöglichen Behörden die Integration von Domänen für eine verbesserte Zusammenarbeit und Entscheidungsfindung.

Ereignis- und Vorfallmanagement

Das IBM Intelligent Operations Center stellt einen Mechanismus für die Erstellung von Ereignisberichten und ein Überwachungsverfahren zur Verfügung, mit denen Störungen über die zugrunde liegenden Domänen hinweg erkannt werden können und ein Einblick in diese Störungen ermöglicht wird. Sie können vorhergesagte Ereignisse, geplante Ereignisse und aktuelle Ereignisse im Verlauf ihrer Entstehung verwalten. Der Austausch von Leitungen, die unter einer Straße verlaufen, ist beispielsweise ein geplantes Ereignis oder ein geplanter Auftrag mit einer Auswirkung auf die Wasserversorgung und den Verkehr. Schlechtes Wetter, das für die nächsten 24 Stunden angekündigt ist, ist ein vorhergesagtes Ereignis. Ein Verkehrsstau ist ein aktuelles Ereignis, das sowohl durch Straßenarbeiten als auch durch das Wetter beeinflusst wird.

Ein integriertes geografisches Informationssystem (GIS) oder eine Positionskarte ordnet Ereignisse grafisch zu, was Ihnen die Einschätzung der Auswirkung von Ereignissen durch eine interaktive Zuordnung und Szenarioanalyse ermöglicht.

Ressourcen-, Reaktions- und Aktivitätenverwaltung

IBM Intelligent Operations Center stellt ein System bereit, mit dem Sie die entsprechenden Verfahren und Workflows anhand der zu Ereignissen zugehörigen Aktivitäten speichern können. Sie können den Fortschritt der Workflows protokollieren und überwachen oder den Status der Ihnen zugewiesenen Aktivitäten aktualisieren.

Informationen zu einem Bereich verfügbarer Ressourcen können auf einer Karte hervorgehoben werden. Auf diese Informationen können Sie bei Bedarf jederzeit und von überall zugreifen.

Statusüberwachung

Das IBM Intelligent Operations Center stellt ein Tool für die Erstellung und Anzeige von KPIs zur Verfügung. Die KPIs können als zugrunde liegende Datenänderungen aktualisiert werden. Mit diesem Tool haben Sie folgende Möglichkeiten:

- Zusammenfassung des Status auf Führungsebene für eine einzelne Domäne oder für mehrere Domänen
- Hervorhebung und Erkennung von Problemen
- Nähere Untersuchung durch Drilldownoperationen in KPI-Details

Sofortige Benachrichtigung und Echtzeitkommunikation

Das IBM Intelligent Operations Center stellt einen Arbeitsbereich zur Verfügung, in dem Sie Alerts für Angelegenheiten pflegen können, die besondere Aufmerksamkeit erfordern. In diesem Arbeitsbereich können Sie Neuigkeiten und Ereignisse überwachen, was vor allem hilfreich ist, wenn sonstige Portlets, die Neuigkeiten melden, nicht in der Ansicht enthalten sind.

IBM Lotus Sametime stellt ein integriertes Tool für die Onlinezusammenarbeit und Kommunikation zur Verfügung, das sie bedarfsgerecht gezielt an bestimmten Stellen für Sofortnachrichten verwenden können.

Berichte erstellen

Das IBM Intelligent Operations Center beinhaltet eine integrierte Berichtsfunktion, sodass Sie Berichte mit den von der Lösung bereitgestellten Ereignissen und KPIs einrichten und ausführen können. Mit dieser Funktion können Sie die für Sie nützlichsten Informationen aktuell und regelmäßig sammeln und darstellen. Diese Funktionen bietet Ihnen alle Vorteile angepasster Zusammenfassungen und Diagramme.

Benutzer und Leistungen

Das IBM Intelligent Operations Center wurde für Personal entwickelt, das sich mit der Betriebssteuerung in Unternehmen, staatlichen Stellen oder kommunalen oder städtischen Ämtern befasst: Entscheidungsträger, Aufsichtspersonen und Betreiber.

In der folgenden Tabelle werden die Benutzer und Vorteile beschrieben, die mit der Verwendung des IBM Intelligent Operations Center in Zusammenhang stehen.

Tabelle 1. IBM Intelligent Operations Center - Benutzer und Vorteile

Ihr Aufgabengebiet	**Diese Software unterstützt Sie bei folgenden Aufgaben:**
Entscheidungsträger	• Erhalt einer Zusammenfassung auf Führungsebene, die sich mit Ereignissen und Vorfällen befasst und über Karten, Dashboards und Alerts gewonnen wird • Bestimmung von Kennzahlen für den organisatorischen Erfolg mithilfe von Key Performance Indicators (KPIs) • Erkennung und Überwachung von Problemen mithilfe von Berichten • Festlegung der Prioritäten und Implementierung einer Richtlinie anhand der bereitgestellten Daten
Aufsichtsperson	• Erkennung von auf Karten, in Dashboards und Alerts angezeigten Konflikten und Problemen sowie Ergreifung entsprechender Gegenmaßnahmen • Ereignisverwaltung durch das Hinzufügen neuer Ereignisse, Bearbeiten bereits vorhandener Ereignisse, Abbrechen von Ereignissen und Eskalieren von Ereignissen zur Ausweisung als Vorfälle • Bereitstellung von Informationen zu und Verwalten von Ressourcen • Speichern und Verwalten der Ausführung von Prozeduren und Workflows, die Ereignissen zugeordnet sind • Überwachung von KPIs • Schnelle und unkomplizierte Weiterleitung von wichtigen Angelegenheiten • Entwurf sinnvoller Berichte
Betreiber	• Erstellung, Bearbeitung und Statusüberwachung von Ereignissen und Vorfällen für die Anzeige in entsprechenden Listen • Erhalt und Aktualisierung des Status für zugeordnete Aktivitäten • Überprüfen verfügbarer Ressourcen • Ausführen regelmäßiger und aktueller Berichte • Benachrichtigung, Aktualisierung und Ausgeben von Alerts an entsprechende Kollegen, Manager oder Vorgesetzte • Schnelle und unkomplizierte Kommunikation im Notfall und in sonstigen Situationen, die eine Reaktion erfordern
Benutzeradministrator	• Hinzufügen neuer Benutzer und deren Zuordnung zu Gruppen mit der entsprechenden Authentifizierung • Gewährleistung der Datensicherheit durch kategorie- und rollenbasierte Berechtigungsgruppen mit entsprechenden Berechtigungen • Gezielte Einrichtung von Berechtigungen für Fachgebiete und erforderliche Daten

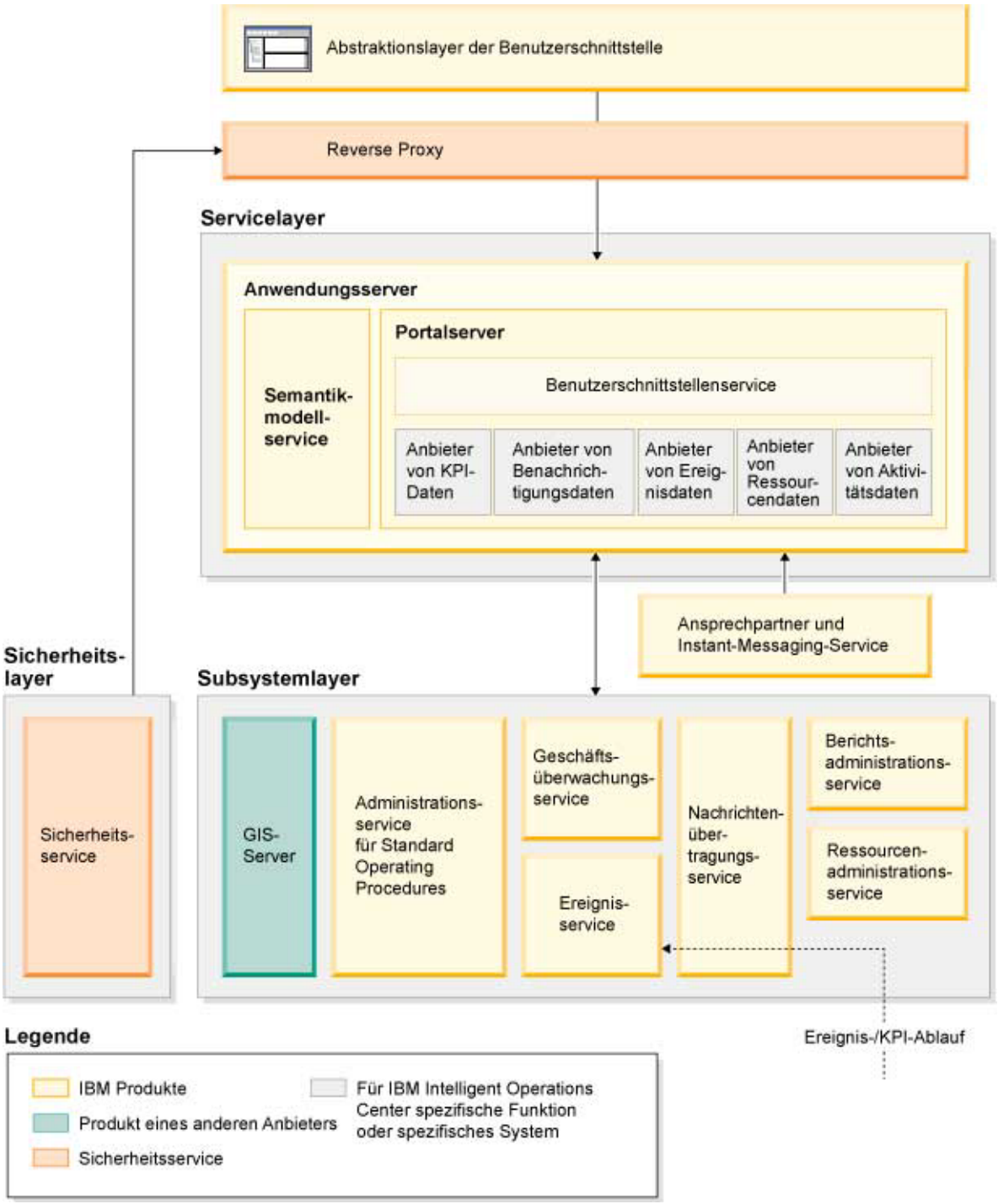
Tabelle 1. IBM Intelligent Operations Center - Benutzer und Vorteile (Forts.)

Ihr Aufgabengebiet	**Diese Software unterstützt Sie bei folgenden Aufgaben:**
Systemadministrator	• Anpassen von Seiten und Portlets an die Anforderungen des Unternehmens • Anpassen der angezeigten Ereignisse und KPIs entsprechend den Managementanforderungen • Erstellen und Veröffentlichen von Testereignissen • Konfigurieren von Berichten und deren Verteilung

Komponenten

Auf übergeordneter Ebene lässt sich die Struktur des IBM Intelligent Operations Center in Hauptkomponenten, Subsysteme und Services unterteilen.

Das folgende Diagramm zeigt eine übergeordnete Ansicht von IBM Intelligent Operations Center.



Abstraktionslayer der Benutzerschnittstelle

Das IBM Intelligent Operations Center bietet webbasierte Portale, in denen Ereignisdaten, der Gesamtstatus und Details gebündelt zur Verfügung stehen. Die Benutzerschnittstelle stellt angepasste Informationen in verschiedenen vorkonfigurierten Ansichten und in einheitlichen Formaten dar. Sämtliche Informationen werden über benutzerfreundliche Dashboards angezeigt.

Sicherheitslayer

Der gesamte Informationszugriff wird durch den Sicherheitslayer mithilfe von Organisationsrollen und Datenkategorien gesteuert. Diese Steuerung verhindert einen unbefugten Zugriff und ermöglicht gleichzeitig eine einfache Verwaltung der Berechtigungen.

Servicelayer

Der Servicelayer verwendet einheitliche Widgets und eine einheitliche Rahmendefinition für Benutzerschnittstellenservices, um Ereignisdaten zu empfangen und diese über das Ereignismanagement an das Nachrichtensystem zu übergeben. IBM Intelligent Operations Center-Datenlieferanten erweitern die Benutzerschnittstellenservices. Aufgrund der Vielfalt an Daten, die aus den zugrunde liegenden betrieblichen Systemen bereitgestellt werden können, werden die Daten anhand eines Referenzmodells mit Standardsemantik normalisiert. Dieses bietet ein einheitliches Verzeichnis für die Zuordnung von Beziehungen. Dieses Modell erleichtert die Auswirkungsanalyse und die Reaktion auf Ereignisse, da die Informationen nicht mehrmals umgewandelt werden müssen. Das Semantikmodell stellt den Zugriff auf KPI-Informationen und Hierarchiedaten der zugrunde liegenden Domänen zur Verfügung. Für Daten kann eine erweiterte Analyse durchgeführt werden, damit Optimierungen und Vorhersagen bestimmt werden können, die zur Entscheidungsfindung und Governance herangezogen werden können.

Subsystemlayer

Die Lösung stellt einen Mediationslayer zur Verfügung, mit dem der Datenaustausch zwischen der Lösung und den betrieblichen Systemen der zugrunde liegenden Domänen erleichtert wird. Daten aus verschiedenen konfigurierbaren Quellen können über Gateways in einem Subsystemlayer bereitgestellt werden, der Alerts, KPIs und Ereignisse generieren kann. Dieser Integrationslayer ermöglicht die wechselseitige Übertragung von Nachrichten in verschiedenen Formaten, wobei im Idealfall offene Standards verwendet werden. Da die Quellendaten mithilfe branchenüblicher Tools in das Referenzsemantikmodell konvertiert werden, ist keine Änderung der zugrunde liegenden betrieblichen Systeme erforderlich. Notfallsysteme und sonstige Reaktionssysteme können zur Einleitung geeigneter Workflows mit dem IBM Intelligent Operations Center verbunden werden.

Die Struktur des IBM Intelligent Operations Center unterstützt Folgendes:

- Eine zentrale Stelle, über die Sie einen Einblick in den Status von Operationen erhalten, Ereignisse und Vorfälle verwalten und Domänen unter der Steuerung des Operations Center verbinden können.
- Die Integration mit einem geografischen Informationssystem (GIS), einem Positionskartendiagramm oder einem Plan für die räumliche und grafische Zuordnung von Ereignissen, Vorfällen und Ressourcen
- Die Erstellung und Überwachung von Key Performance Indicators (KPIs), die durch Verbindungen mit zugrunde liegenden Domänensystemen als Datenänderungen aktualisiert werden
- Die Erstellung und Überwachung der Standard Operating Procedures (SOPs) mit Workflows und Aktivitäten in Verbindung mit Ereignissen
- Alerts, die von den Außenstellen eingehen. Dazu zählen auch Alerts, die Notfall- oder Standardreaktionen erfordern.
- Funktionen für die Onlinezusammenarbeit über eine Instant Messaging-Funktion mit IBM Lotus Sametime

- Erstellung und Verteilung von aktuellen und regelmäßigen Berichten anhand von Ereignis- oder KPI-Daten
- Ein rollenbasiertes Sicherheitsmodell

Weitere Informationen zu den IBM Intelligent Operations Center-Systemservices erhalten Sie über den Link am Ende des Themas.

Zugehörige Konzepte:

„IBM Intelligent Operations Center-Systemservices" auf Seite 13
IBM Intelligent Operations Center-Server stellen eine Reihe von Services bereit.

Ereignismanagement

Die IBM Intelligent Operations Center-Lösung ist spezialisiert auf die Integration und Optimierung von Informationen innerhalb von und zwischen Domänen in einem Operationshub. Dies geschieht in Echtzeit oder über einen langen Zeitraum. Das Ereignisdatenmanagement ermöglicht es IBM Intelligent Operations Center, Daten von mehreren Systemen aufzunehmen, um signifikante Ereignisse und Trends konstant vorherzusagen und auf sie zu reagieren.

Ereignisnachrichten sind eigenständige Datenelemente, die grundlegende, aber vollständige Informationen enthalten, auf die Empfänger reagieren können. Ereignisnachrichten werden vom IBM Intelligent Operations Center in Warteschlangen angeordnet und vom Ereignisverarbeitungsservice verarbeitet.

Ereignisse gehen in unterschiedlicher Form in das IBM Intelligent Operations Center ein, je nach Art der Vorgänge und Domänen im zentralen Operationshub. Beispiele für Ereignisformen sind: Trigger, Schwellenwerte, komplexe Ereignisse und manuell generierte Ereignisse.

Trigger sind Ereignisse, die durch ein Geschehnis generiert werden, und erfordern i. d. R. eine Aktion des Empfängers. Zu den Triggern zählen:

- Ausgelöster Feueralarm oder Rauchmelder
- Abstürzende IT-Systeme
- Ausgelöste Detektoren für Angriffe von außen
- Von Sensoren wahrgenommene Naturereignisse wie Erdstöße

Das IBM Intelligent Operations Center kann Informationen zu solchen Ereignissen von externen Systemen empfangen und in Alerts für Empfänger konvertieren. In der Regel ist es wahrscheinlich, dass Indikatoren einer niedrigeren Ebene zusammengefasst werden und nur dann an das IBM Intelligent Operations Center übermittelt werden, wenn sie einer größeren Aufmerksamkeit bedürfen. So werden z. B. möglicherweise nicht alle Brände als Ereignisse berichtet. Wenn Brände jedoch mehrere Bereiche der Feuerwehr betreffen und, aufgrund von Gefahrgut, Fachwissen im Bereich des Umweltschutzes erfordern, würde dies einen Bericht an die Einsatzzentrale begründen.

Schwellenwertereignisse helfen Ihnen dabei, zu bestimmen, wann die von einem Sensor oder einer anderen Quelle erhaltenen Messwerte den normalen Bereich verlassen haben. Grundlegende Schwellenwertereignisse gleichen mindestens zwei Messwerte miteinander ab und berichten über einen Trend. Komplexere Schwellenwertereignisse können Messwerte mit einem Schwellenwert abgleichen, der mit historischen Informationen erstellt wurde. Zu den Schwellenwerten zählen:

- Alarme bei zu hoher oder zu niedriger Temperatur
- Hohe oder niedrige Wasserstände
- Luft- und Wasserqualität, die nicht den Umweltstandards entspricht
- Übermäßiger Stromverbrauch

Das IBM Intelligent Operations Center kann solche Ereignisse in Form von wesentlichen Leistungsindikatoren (Key Performance Indicators, KPIs) verwalten.

Komplexe Ereignisse verbinden Informationen von mehreren Systemen, um zu bestimmen, ob eine Gruppe in Verbindung stehender Ereignisse gemeldet werden sollte. Dies ist z. B. der Fall, wenn die Mautbehörde ein Triggerereignis empfängt, das angibt, dass der Computeranschluss für Kreditkartenautorisierung nicht funktioniert, und kurz darauf ein Schwellenwertereignis des Finanzsystems eingeht, das eine Warnung ausgibt, weil sein Kreditlimit für nicht autorisierte Zahlungen beinahe erreicht ist. Die Kombination dieser beiden Probleme ist viel ernster als eines der beiden alleine. Deshalb wird ein komplexes Ereignis generiert, um die Aufmerksamkeit zu erhöhen und eine Problemlösung zu koordinieren.

Manuell eingegebene Ereignisse sind für Städte von besonderer Bedeutung. Hierzu zählen beobachtete Zwischenfälle wie Verbrechen und Verkehrsunfälle. Andere Beispiele für manuell eingegebene Ereignisse sind durch Notrufe von Bürgern, Berichte von städtischen Beamten oder Managementsysteme generierte Ereignisse, die über den Zustand der Stadt berichten. Zu den häufigsten manuell eingetragenen Ereignissen zählen:

- Unwetterwarnungen
- Verbrechensmeldungen
- Brände
- Vorfälle im Straßenverkehr – Unfälle, Staus, Sondertransporte
- Bevorstehende Veranstaltungen – Rockkonzerte, Straßenrennen, Umzüge

Die Verarbeitung komplexer Ereignisse ermöglicht es einer Stadt, auf einfache Weise Abweichungen vom Stadtsystem festzustellen, gelegentlich mithilfe von nicht zusammengehörigen Daten Trends zu erkennen und zukünftige Probleme vorherzusagen.

Neuerungen in Version 1.5

IBM Intelligent Operations Center 1.5 bietet eine Einführung in hilfreiche neue Funktionen für Administratoren und Benutzer.

Neuerungen für den Benutzer

Mit IBM Intelligent Operations Center 1.5 können Sie zu einem Ereignis gehörende Ressourcen und Aktivitäten verwalten.

Ressourcen verwalten und mit Positionskarten interagieren

In den neuen und erweiterten Portlets Positionskarte und Karte können Sie folgende Schritte durchführen:

- Die in der Nähe eines Ereignisses verfügbaren Ressourcen anhand einer geografischen Karte bewerten.
- Mit einem neuen Kartentyp, der Positionskarte, mit definierten interaktiven Bereichen arbeiten. Eine Positionskarte kann beispielsweise auf einem Routenplan für ein Transportsystem basieren.
- Mehrere Ereignisse an derselben Position auf einer Karte anzeigen.

 Weitere Informationen zum neuen Positionskarte-Portlet und zur Karte-Verbesserung sowie zu den Details-Portlets erhalten Sie über die Links am Ende des Themas.

Den Status von zu Ereignissen gehörenden Aktivitäten protokollieren

Im neuen Portlet Meine Aktivitäten können Sie folgende Aktionen ausführen:

- Die einem Verfahren und einem Ereignis zugeordneten offenen Tasks für Ihre Gruppe anzeigen.
- Den Status der Ihnen zugewiesenen Tasks anzeigen.
- Den Status der Ihnen zugewiesenen Tasks ändern.

Weitere Informationen zum Meine Aktivitäten-Portlet erhalten Sie über den Link am Ende des Themas.

Berichte erstellen

Im neuen Portlet Berichte können Sie folgende Aktionen ausführen:

- Maximal sechs Berichte zu Ereignissen als Diagramme darstellen.
- Benutzerdefinierte Berichte anhand ausgewählter Kriterien und Daten erstellen. Dazu gehören auch Berichte für Ereignisse nach Datum oder Datumsbereich.
- Eine Berichts-URL kopieren und den Bericht in einem Teilfenster auf der rechten Seite des Portlets anzeigen.

Weitere Informationen zum Berichte-Portlet erhalten Sie über den Link am Ende des Themas.

Zugehörige Konzepte:

„Positionskarte” auf Seite 291
Mit dem Portlet "Positionskarte" können Sie die auf einer Positionskarte markierten Ereignisse anzeigen. Eine Positionskarte im IBM Intelligent Operations Center ist eine Karte oder ein Plan mit vordefinierten Interaktionsbereichen, wie z. B. Sitzbereiche in großen Sportstadien.

„Karte” auf Seite 294
Mit dem Portlet "Karte" können Sie die in einer Karte enthaltenen Ereignisse und Ressourcen anzeigen.

„Details” auf Seite 287
Mit dem Portlet "Details" können Sie in IBM Intelligent Operations Center Ereignisse anzeigen, überwachen und verwalten.

„Meine Aktivitäten” auf Seite 300
Im Portlet "Meine Aktivitäten" wird eine dynamische Liste mit Aktivitäten angezeigt, deren Eigner die Gruppe ist, zu der der an der Schnittstelle angemeldete Benutzer gehört.

„Berichte” auf Seite 304
Mit dem Portlet "Berichte" können Berichte von Ereignissen in Form von Diagrammen angezeigt werden. In diesem Portlet gibt es mehrere Möglichkeiten für die Anordnung von Ereignissen; darüber hinaus können Ereignisse nach einem bestimmten Datum oder Zeitraum ausgewählt werden. Mithilfe dieser Berichte können Sie Maßnahmen für aktuelle und künftige Ereignisse planen.

Neuerungen für den Administrator

Ab Version 1.5 können Sie Ihre Portlets und Seitenlayouts anpassen. Sie können zudem Standard Operating Procedures und Workflows konfigurieren.

Portlets anpassen

Mit den neuen Portletkonfigurationsoptionen können Sie für jedes Portlet folgende Elemente festlegen:

- Eigenschaften, die nur für einzelne Portlets gelten, beispielsweise das Festlegen von Mittelpunkt und Zoomstufe für eine Karte
- Eigenschaften, die generell für alle Portlets gelten, beispielsweise das Festlegen der Portlethöhe

Weitere Informationen zum Anpassen von Portlets erhalten Sie über den Link am Ende des Themas.

Ereignisse mit Standard Operating Procedures und Workflows verwalten

Sie können zu Ereignissen zugehörige Verfahren und Aktivitäten definieren:

- Standard Operating Procedures auf Basis eines Arbeitsplans definieren.
- Workflows erstellen.

- Parameter für die Auswahl einer Standard Operating Procedure auf Basis der Parameter eines Ereignisses definieren.

 Weitere Informationen zum Verbinden von Aktivitäten in Bezug auf Ereignisse erhalten Sie über den Standard Operating Procedure-Link am Ende des Themas.

Scripts erstellen und Ereignisse veröffentlichen

Mit dem neuen Portlet Erstellung von Ereignisscripts können Sie eine sequenzielle Liste von Ereignissen erstellen, die in vordefinierten Zeitabständen veröffentlicht werden soll.

 Weitere Informationen zur Scripterstellung und zur Veröffentlichung von Ereignissen erhalten Sie über den Link am Ende des Themas.

Servicestatus überprüfen

Mit dem neuen Tool Systemprüfung können Sie den Betriebsstatus der IBM Intelligent Operations Center-Services überprüfen.

 Weitere Informationen zum Systemprüfung-Tool erhalten Sie über den Link am Ende des Themas.

Protokolle unterstützen

Das IBM Intelligent Operations Center unterstützt jetzt Ereignisse mit anderen Protokollen als das Common Alerting Protocol. Sie können folgende Schritte durchführen:

- Aufzählungstypen für Common Alerting Protocol- und kein Common Alerting Protocol-Ereignisse erweitern.
- Die Popup-Menüs im Portlet Details anpassen.
- Ereignisse von mehreren Domänen für die Anzeige in Portlets akzeptieren.

 Weitere Informationen zu Integrationspunkten und Protokollen erhalten Sie über den Link am Ende des Themas.

Zugehörige Konzepte:

„Standard Operating Procedures” auf Seite 135
Für die Verwaltung von Ereignissen, die im IBM Intelligent Operations Center auftreten, können Sie Standard Operating Procedures und Aktivitäten definieren. Verwenden Sie das Portlet "Standard Operating Procedures", um auf Standard Operating Procedure, Auswahlmatrix für Standard Operating Procedure und Workflow-Designer-Anwendungen in Tivoli Service Request Manager zuzugreifen.

„Erstellung von Ereignisscripts” auf Seite 114
Mit dem Portlet "Erstellung von Ereignisscripts" können Sie ein Script zum Erstellen einer sequenziellen Liste von Ereignissen schreiben, die nacheinander in vorgegebenen Zeitintervallen veröffentlicht werden sollen.

„Komponenten überprüfen” auf Seite 220
Mit dem Systemprüfungstool wird überprüft, ob auf die Komponenten in IBM Intelligent Operations Center zugegriffen werden kann und ob sie betriebsbereit sind.

„Integrationspunkte und -protokolle” auf Seite 97
Andere Systeme können über die IBM Intelligent Operations Center-Services und -Richtlinien mit der Lösung integriert werden. Daten können im CAP-Format (Common Alerting Protocol) empfangen werden; andere Protokolle werden ebenfalls unterstützt.

Zugehörige Tasks:

„Portlets anpassen” auf Seite 154
Als Administrator können Sie die Portleteinstellungen ändern, um ein Portlet anzupassen.

Kapitel 2. Installation und Konfiguration

IBM Intelligent Operations Center stellt einen Implementierungsassistenten bereit, der die für IBM Intelligent Operations Center erforderliche Umgebung installiert. Nach der Implementierung der Umgebung und des IBM Intelligent Operations Center-Pakets sind einige zusätzliche Konfigurationen erforderlich.

Installation vorbereiten

Bevor Sie IBM Intelligent Operations Center implementieren, machen Sie sich mit der IBM Intelligent Operations Center-Systemkonfiguration vertraut und stellen Sie sicher, dass alle Voraussetzungen für die Umgebung erfüllt sind.

IBM Intelligent Operations Center-Systemservices

IBM Intelligent Operations Center-Server stellen eine Reihe von Services bereit.

Analyseservices
Stellen Datenanalyse- und Präsentationsservices bereit.

Anwendungsserver
Stellen zur Unterstützung des Produkts Services der Java Enterprise Edition bereit.

Sicherheit
Stellen Services bereit, die bestimmen, ob ein Benutzer für die Verwendung des Systems autorisiert ist, und die Berechtigungen der Benutzer innerhalb des Systems definieren.

Berechtigungsservices
Stellen Services bereit, die die Services bestimmen, für deren Verwendung ein Benutzer autorisiert ist.

Geschäftsüberwachung
Stellen Zusammenfassungen, Analysen und Präsentationen von Informationen zu Geschäftsprozessen und -aktivitäten in Echtzeit bereit.

Instant-Messaging-Server
Stellen Funktionen zur Zusammenarbeit für Benutzer und Anwendungen in Echtzeit zur Verfügung.

Konfigurationsservices
Verwalten die Produktkonfiguration, einschließlich dem Bestands- und Änderungsmanagement.

Datenbank
Stellen den Datenbankmanager für Anwendungs- und Systemdaten bereit.

Verzeichnis
Stellen die Zuordnungen zwischen Namen und Werten bereit. Datenservices werden als Repository für Benutzernamen und -kennwörter verwendet.

Ereignisbehandlung
Sammeln, aggregieren, präsentieren und bearbeiten Systemereignisse.

Nachrichtenübertragungsservices
Stellen Nachrichten- und Workflow-Services für das Produkt bereit.

Überwachungsservices und -agenten
Stellen Überwachungsaktivitäten innerhalb des Produkts bereit.

Portal Stellen Services zur Unterstützung der Benutzerinteraktion mit dem Produkt bereit.

Semantikmodell

Stellt Services bereit, die es Anwendungen ermöglichen, Objekte und Beziehungen der realen Welt zu modellieren.

Zugehörige Konzepte:

„Komponenten" auf Seite 6
Auf übergeordneter Ebene lässt sich die Struktur des IBM Intelligent Operations Center in Hauptkomponenten, Subsysteme und Services unterteilen.

IBM Intelligent Operations Center Hardwarevoraussetzungen

Es sind fünf Server erforderlich, die Mindestvoraussetzungen entsprechen, um IBM Intelligent Operations Center zu installieren.

Die Server müssen 64-Bit-x86-Server sein.

Die Server mit den Mindestvoraussetzungen, die von IBM Intelligent Operations Center verwendet werden, sind in Tabelle 2 angezeigt. Der empfohlene Mindestfestplattenspeicher schließt nicht den Speicherplatz für Boot- und Auslagerungspartitionen mit ein.

Tabelle 2. Mindestvoraussetzungen für die Hardware

Ressource	Anwendungs-server	Ereignisserver	Datenserver	Verwaltungs-server	Installations-server
CPUs	4	4	4	4	2
Speicherplatz	24 GB	16 GB	16 GB	24 GB	4 GB
Netzadapter	1	1	1	1	1
Festplattenspeicher	113 GB	108 GB	108 GB	108 GB	108 GB
Während der Installation erforderlicher zusätzlicher Festplattenspeicher	90 GB	90 GB	90 GB	90 GB	90 GB

Die Mindestvoraussetzungen für die Verzeichnisse auf jedem Server, ausschließlich dem für Boot- und Auslagerungspartitionen erforderlichen Speicherbereich, sind in Tabelle 3 angegeben.

Tabelle 3. Mindestvoraussetzungen an Speicherplatz für jedes Verzeichnis

Verzeichnis	Mindestspeicherplatz	Anmerkungen
`/`	8 GB	
`/opt`	35 GB oder 40 GB	Für den Anwendungsserver sind 40 GB erforderlich und 35 GB für alle anderen Server
`/usr`	8 GB	
`/home`	5 GB	
`/tmp`	10 GB	
`/chroot`	1 GB	
`/datahome`	25 GB	
`/loghome`	8 GB	
`/installMedia`	90 GB	Dieses Verzeichnis kann nach der Installation gelöscht werden.
`/var`	8 GB	

Zugehörige Tasks:

„Server vorbereiten" auf Seite 19
Überprüfen Sie vor der Installation von IBM Intelligent Operations Center, ob die Voraussetzungen für die Konfiguration des Servers erfüllt sind. Mithilfe des Vorabprüfungstools wird sichergestellt, dass ein Großteil dieser Voraussetzungen berücksichtigt wurde.

Zugehörige Informationen:

Systemvoraussetzungen

Softwarevoraussetzungen

Vor der Installation von IBM Intelligent Operations Center muss auf den Servern die entsprechende Software installiert sein.

IBM Intelligent Operations Center benötigt eine Installation von Red Hat Enterprise Linux (RHEL) 5 Server x86-64 Update 5 oder höher auf allen Servern. Red Hat Enterprise Linux Version 6 wird nicht unterstützt.

Zugehörige Tasks:

„Server vorbereiten" auf Seite 19
Überprüfen Sie vor der Installation von IBM Intelligent Operations Center, ob die Voraussetzungen für die Konfiguration des Servers erfüllt sind. Mithilfe des Vorabprüfungstools wird sichergestellt, dass ein Großteil dieser Voraussetzungen berücksichtigt wurde.

Zugehörige Informationen:

Systemanforderungen

Unterstützte Browser

Die Schnittstelle für IBM Intelligent Operations Center-Lösungen unterstützt eine Reihe von Browsern. Einige Browser können mit Einschränkungen verwendet werden.

IBM Intelligent Operations Center wurde auf folgenden Browsern getestet und wird von diesen unterstützt:

- Microsoft Internet Explorer 8.x (nur 32-Bit)
- Microsoft Internet Explorer 9.x (nur 32-Bit)
- Mozilla Firefox 10 ESR

Kompatibilitätsansicht von Internet Explorer

IBM Intelligent Operations Center unterstützt die Kompatibilitätsansicht von Internet Explorer 8 oder Internet Explorer 9 nicht.

Anmerkung: Die Kompatibilitätsansicht ist möglicherweise vorübergehend aktiviert, wenn beim Erstellen einer neuen Seite für die Benutzerschnittstelle ein Problem auftritt. Weitere Informationen dazu erhalten Sie über den Link am Ende des Themas.

Durchsatz von Internet Explorer 8.x

Möglicherweise müssen Benutzer bei Verwendung Internet Explorer 8.x eine langsame Verarbeitung in Kauf nehmen.

Um dieses Problem zu vermeiden, verwenden Sie Internet Explorer 9.x oder Firefox 10 ESR.

Minimale Bildschirmauflösung

IBM Intelligent Operations Center ist für eine Bildschirmauflösung von mindestens 1280 x 800 ausgelegt.

Zugehörige Tasks:

„Neue Seite für die Benutzerschnittstelle kann nicht erstellt werden" auf Seite 350
Beheben Sie ein Problem, das beim Erstellen einer neuen Seite auftritt, wenn Sie mit Microsoft Internet Explorer 9 arbeiten.

Paketierung der Datenträger

IBM Intelligent Operations Center kann als Paket mit DVDs bestellt werden oder über Passport Advantage bezogen werden.

Die Produktnummer lautet 5725-D69.

Zugehörige Informationen:

Passport Advantage

Laden Sie die Imagedateien für IBM Intelligent Operations Center Version 1.5 herunter

---

Installationsprüflisten

Es sind Installationsprüflisten für die beiden unterschiedlichen Installationsoptionen für IBM Intelligent Operations Center verfügbar. Diese Prüflisten bieten einen Überblick über die Installationsschritte und können für die Überwachung des Installationsfortschrittes verwendet werden.

Prüfliste - Installation mithilfe des IBM Installation Manager

Verwenden Sie diese Prüfliste, um die Installationsschritte nachzuverfolgen, wenn Sie IBM Intelligent Operations Center mithilfe vonIBM Installation Manager installieren.

Informationen zu diesem Vorgang

Eine druckbare Version dieser Prüfliste erhalten Sie über den entsprechenden Link am Ende dieses Themas.

Vorgehensweise

__ 1. Stellen Sie sicher, dass Sie über die nötige Hardware verfügen.
__ 2. Stellen Sie sicher, dass die erforderliche Software auf der Hardware installiert ist.
__ 3. Bereiten Sie die Server vor.
__ 4. Kopieren Sie das Installationspaket auf den Installationsserver.
__ 5. Installieren Sie Java Runtime Environment.
__ 6. Installieren Sie IBM Installation Manager.
__ 7. Starten Sie IBM Installation Manager neu und installieren Sie das Paket **Topologie konfigurieren**.
__ 8. Starten Sie IBM Installation Manager neu und installieren Sie das Paket **Zielserver vorbereiten**. Wenn dieser Schritt erfolgreich abgeschlossen ist, überspringen Sie Schritt 9.
__ 9. Starten Sie IBM Installation Manager neu und installieren Sie das Paket **Systemprüffehler ignorieren**. Wenn Sie IBM Installation Manager ausführen, nachdem Sie die Systemprüffehler behoben haben, oder nachdem Sie bestimmt haben, dass die Installation fortgesetzt werden kann, wählen Sie für das zweite Ausführen **Zielserver vorbereiten** und **Systemprüfungsfehler ignorieren** aus.
__ 10. Starten Sie IBM Installation Manager neu und installieren Sie das Paket **Umgebung vorbereiten**.
__ 11. Starten Sie IBM Installation Manager neu und installieren Sie das Paket **Plattform installieren und konfigurieren - Teil 1**.

Tipp: Wählen Sie nicht Teil 1 und Teil 2 gleichzeitig aus. Die Ausführung dieser Schritte nimmt die meiste Zeit in Anspruch. Wenn beide gleichzeitig ausgeführt werden und es zu einem Fehler kommt, müssen beide erneut ausgeführt werden. Das gilt selbst dann, wenn einer der Teile erfolgreich war.

Wichtig: Schalten Sie die Server zwischen den Installationsphasen nicht herunter. Das Herunterfahren von Servern zwischen Installationsphasen wurde nicht getestet und kann zu unvorhersehbaren Ergebnissen führen.

__ 12. Starten Sie IBM Installation Manager neu und installieren Sie das Paket **Plattform installieren und konfigurieren - Teil 2**.

__ 13. Starten Sie IBM Installation Manager neu und installieren Sie das Paket **Plattformsteuerungstool installieren**.

__ 14. Starten Sie IBM Installation Manager neu und installieren Sie das Paket **Systemprüfungstool installieren**.

__ 15. Starten Sie alle IBM Intelligent Operations Center-Server neu.
   a. Fahren Sie alle IBM Intelligent Operations Center-Server mithilfe des Plattformsteuerungstools herunter.
   b. Fahren Sie alle Server herunter und starten Sie sie über das Betriebssystem neu.
   c. Starten Sie alle IBM Intelligent Operations Center-Server mithilfe des Plattformsteuerungstools.

__ 16. Starten Sie IBM Installation Manager neu und installieren Sie das Paket **Anwendung installieren**. Dadurch wird die IBM Intelligent Operations Center-Anwendung installiert.

__ 17. Konfigurieren Sie die IBM Intelligent Operations Center-Architektur.
   __ a. Wenn Sie IPv6 verwenden, konfigurieren Sie Services zur Zusammenarbeit.
   __ b. Konfigurieren Sie Single Sign-on für Services zur Zusammenarbeit.
   __ c. Installieren und konfigurieren Sie Semantic Model Services.
   __ d. Konfigurieren Sie das Plattformsteuerungstool.
   __ e. Verschlüsseln Sie das administrative Kennwort für Tivoli Service Request Manager.
   __ f. Legen Sie die Mindestanzahl von Threads für den Ereignisprozessor fest.
   __ g. Ändern Sie die Größe des Standard-Thread-Pools und des Web-Container-Thread-Pools.

__ 18. Installieren Sie alle weiteren Anwendungen.

__ 19. Starten Sie IBM Installation Manager neu, installieren Sie das Paket **Cyber Hygiene** und führen Sie es aus. Cyber Hygiene bietet zusätzliche Sicherheit für das IBM Intelligent Operations Center-System.

Anmerkung: Cyber Hygiene wird innerhalb desselben Schrittes installiert und ausgeführt.

__ 20. Konfigurieren Sie Benutzer, die einen SSH-Zugriff und Kennwörter benötigen.

Ergebnisse

Die IBM Intelligent Operations Center-Architektur und IBM Intelligent Operations Center-Anwendung sind installiert und einsatzbereit.

Nächste Schritte

Ein MustGather-Tool wird bereitgestellt, um Installationsprotokolle zu sammeln, die bei der Diagnose von Installationsproblemen hilfreich sein können.

Zugehörige Konzepte:

„Übersicht über Cyber Hygiene" auf Seite 87
Das IBM Intelligent Operations Center-Feature Cyber Hygiene stellt Services bereit, um gegen potenzielle Sicherheitsrisiken im installierten System vorzugehen.

Zugehörige Informationen:

 Druckbare Version dieser Prüfliste

Prüfliste - Schrittweise Installation

Verwenden Sie diese Prüfliste, um die Installationsschritte nachzuverfolgen, wenn Sie IBM Intelligent Operations Center mithilfe von Scripts und Befehlen installieren.

Informationen zu diesem Vorgang

Eine druckbare Version dieser Prüfliste erhalten Sie über den entsprechenden Link am Ende dieses Themas verfügbar.

Vorgehensweise

__ 1. Stellen Sie sicher, dass Sie über die nötige Hardware verfügen.
__ 2. Stellen Sie sicher, dass die erforderliche Software auf der Hardware installiert ist.
__ 3. Bereiten Sie die Server vor.
__ 4. Installieren Sie Java Runtime Environment.
__ 5. Kopieren Sie das Installationspaket auf den Installationsserver.
__ 6. Extrahieren Sie das Installationspaket, und bereiten Sie es vor.
__ 7. Definieren Sie die Installationseigenschaften.
__ 8. Definieren Sie die Topologie für die Installation durch Bearbeiten der Datei mit den Topologieeigenschaften.
__ 9. Generieren Sie das Topologiekennwort, das für die Verschlüsselung von Schlüsseldateien verwendet wird.
__ 10. Generieren Sie die Topologiedatei.
__ 11. Führen Sie das Vorabprüfungstool aus, um zu überprüfen, ob die Umgebung bereit für die Installation von IBM Intelligent Operations Center ist.
__ 12. Konfigurieren Sie Linux-Sicherheitseinstellungen mithilfe des bereitgestellten Tools oder durch Ausführung einer Reihe von Befehlen.
__ 13. Installieren Sie die IBM Intelligent Operations Center-Architektur. Dies kann in einer oder in drei Phasen durchgeführt werden. Wenn Sie die Installation in einer virtualisierten Umgebung ausführen, ermöglicht die Installation in mehreren Phasen Ihnen die Erstellung einer Momentaufnahme zwischen den Installationsphasen.
    - Installieren Sie IBM Intelligent Operations Center in einer Phase. Der Installationsprozess dauert bis zu 14 Stunden.
    - Installieren Sie IBM Intelligent Operations Center in drei Phasen. Die drei Phasen sind:
        a. Kopieren der Installationsdateien vom Installationsserver auf die Zielserver. Diese Phase dauert ungefähr 2 Stunden.
        b. Installieren der ersten Phase der Topologie. Diese Phase dauert ungefähr 9 Stunden.
        c. Installieren der zweiten Phase der Topologie. Diese Phase dauert ungefähr 3 Stunden.

    Wichtig: Schalten Sie die Server zwischen den Installationsphasen nicht herunter. Das Herunterfahren von Servern zwischen Installationsphasen wurde nicht getestet und kann zu unvorhersehbaren Ergebnissen führen.
__ 14. Installieren Sie das Plattformsteuerungstool.

__ 15. Installieren Sie das Systemprüfung Tool.
__ 16. Überprüfen Sie, ob die IBM Intelligent Operations Center-Architektur ordnungsgemäß installiert ist.
__ 17. Konfigurieren Sie die IBM Intelligent Operations Center-Architektur.
    __ a. Wenn Sie IPv6 verwenden, konfigurieren Sie Services zur Zusammenarbeit.
    __ b. Konfigurieren Sie Single Sign-on für Services zur Zusammenarbeit.
    __ c. Installieren und konfigurieren Sie Semantic Model Services.
    __ d. Verschlüsseln Sie das administrative Kennwort für Tivoli Service Request Manager.
    __ e. Legen Sie die Mindestanzahl von Threads für den Ereignisprozessor fest.
    __ f. Ändern Sie die Größe des Standard-Thread-Pools und des Web-Container-Thread-Pools.
__ 18. Installieren Sie die Anwendung IBM Intelligent Operations Center.
__ 19. Installieren Sie alle weiteren Anwendungen.
__ 20. Installieren Sie Cyber Hygiene, und führen Sie es aus. Cyber Hygiene bietet zusätzliche Sicherheit für das IBM Intelligent Operations Center-System.

    Anmerkung: Cyber Hygiene wird innerhalb desselben Schrittes installiert und ausgeführt.
__ 21. Konfigurieren Sie Benutzer, die einen SSH-Zugriff und Kennwörter benötigen.

Ergebnisse

Die IBM Intelligent Operations Center-Architektur und IBM Intelligent Operations Center-Anwendung sind installiert und einsatzbereit.

Nächste Schritte

Ein MustGather-Tool wird bereitgestellt, um Installationsprotokolle zu sammeln, die bei der Diagnose von Installationsproblemen hilfreich sein können.

Zugehörige Konzepte:

„Übersicht über Cyber Hygiene” auf Seite 87
Das IBM Intelligent Operations Center-Feature Cyber Hygiene stellt Services bereit, um gegen potenzielle Sicherheitsrisiken im installierten System vorzugehen.

Zugehörige Informationen:

 Druckbare Version dieser Prüfliste

Server vorbereiten

Überprüfen Sie vor der Installation von IBM Intelligent Operations Center, ob die Voraussetzungen für die Konfiguration des Servers erfüllt sind. Mithilfe des Vorabprüfungstools wird sichergestellt, dass ein Großteil dieser Voraussetzungen berücksichtigt wurde.

Informationen zu diesem Vorgang

Wenn die Installation in einer virtualisierten Umgebung ausgeführt wird, kann die Rüstzeit mithilfe einer Vorlage verkürzt werden.

Vorgehensweise

1. Stellen Sie sicher, dass die Server die Hardware- und Softwareanforderungen erfüllen.
2. Richten Sie ein TCP/IP-Netz ein.
    a. Definieren Sie mithilfe eines DNS-Servers oder durch Definition in der Datei `/etc/hosts` einen vollständig qualifizierten Namen und kurzen Hostnamen.

b. Überprüfen Sie die TCP/IP-Konfiguration. Die Server sind ordnungsgemäß konfiguriert, wenn die folgenden Tests erfolgreich abgeschlossen werden.
   1) Der Befehl **hostname -s** gibt den für den Server definierten kurzen Hostnamen zurück.
   2) Der Befehl **hostname -f** gibt den vollständig qualifizierten Domänen- und Hostnamen für den Server zurück.
   3) Das Ergebnis eines **ping**- oder eines **ping6**-Befehls (für IPV6-Umgebungen) mit den kurzen Hostnamen für die einzelnen Server weist darauf hin, dass auf den Server zugegriffen werden kann.
   4) Das Ergebnis eines **ping**- oder eines **ping6**-Befehls (für IPV6-Umgebungen) mit den vollständig qualifizierten Hostnamen für die einzelnen Server weist darauf hin, dass auf den Server zugegriffen werden kann.
c. Aktivieren Sie die lokale Prüfschleifenadressierung für jeden Server in der Datei `/etc/hosts`.
d. Überprüfen Sie die lokale Prüfschleifenadressierung. Die Server sind ordnungsgemäß konfiguriert, wenn die folgenden Tests erfolgreich abgeschlossen werden.
   1) Der Befehl **ping -n localhost** gibt die Adresse `127.0.0.1` zurück.
   2) Der Befehl **ping -n localhost.localdomain** gibt die Adresse `127.0.0.1` zurück.
   3) Der Befehl **ping6 -n localhost6** in einer IPV6-Umgebung gibt die Adresse `::1` zurück.
   4) Der Befehl **ping6 -n localhost6.localdomain6** in einer IPV6-Umgebung gibt die Adresse `::1` zurück.
e. Stellen Sie sicher, dass die für IBM Intelligent Operations Center erforderlichen Ports verfügbar sind. Die für jeden Server erforderlichen Ports sind in Tabelle 4 angegeben.

Tabelle 4. Für die Produktverwendung erforderliche Ports

Server	Für die Produktverwendung erforderliche Ports
Anwendungsserver	80, 82, 389, 390, 443, 2814, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7234, 7276, 7278, 7279, 7280, 7281, 7283, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 8008, 8880, 8882, 8883, 8885, 8887, 8889, 8890, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9060, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9357, 9359, 9361, 9363, 9364, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9449, 9633, 9634, 9635, 9636, 9638, 9640, 9641, 9810, 9811, 9812, 9813, 9814, 9815, 10000, 10001, 10002, 10003, 10004, 10005, 10006, 10007, 10008, 10009, 10010, 10011, 10012, 10013, 10014, 10015, 10016, 10017, 10025, 10026, 10027, 10028, 10029, 10030, 10031, 10032, 10033, 10034, 10035, 10036, 10037, 10038, 10039, 10040, 10041, 10042, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016
Ereignisserver	80 82, 84, 389, 390, 1414, 8008, 9060, 9080, 20000, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016
Datenserver	389, 390, 50000, 50001, 50002, 50003, 50004, 50005, 50006, 50007, 50008
Verwaltungsserver	80, 82, 389, 390, 1098, 1099, 1527, 1918, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7135, 7136, 7137, 7276, 7278, 7279, 7280, 7282, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 7293, 8008, 8880, 8882, 8884, 8886, 8888, 8890, 8892, 9043, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9358, 9360, 9362, 9364, 9366, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9448, 9449, 9633, 9634, 9635, 9637, 9639, 9641, 9643, 9810, 9811, 9812, 9813, 9814, 9815, 9816, 13100, 13101, 13104, 41001, 50001

f. Stellen Sie sicher, dass die durch den Parameter **nofile** in der Datei `/etc/security/limits.conf` definierten Deskriptoren für maximal geöffnete Dateien für die folgenden Server auf 20480 gesetzt sind:
   - Anwendungsserver
   - Ereignisserver
   - Datenserver
   - Verwaltungsserver

   Fügen Sie dazu der Datei `/etc/security/limits.conf` die folgenden Zeilen hinzu:

```
*   soft   nofile      20480
*   hard   nofile      20480
```

   Dadurch wird die "weiche" Grenze (Standard) für die Anzahl der geöffneten Dateien für alle Benutzer auf 20480 und die "harte" Grenze (maximale Grenzwert) für alle Benutzer auf 20480 festgelegt. Sie können die "harte" Grenze erhöhen, wenn für andere Anwendungen mehr als 20480 Dateien benötigt werden.

g. Fügen Sie den Parameter **net.ipv4.tcp_fin_timeout** hinzu, oder aktualisieren Sie den Parameter in der Datei `/etc/sysctl.conf` für die folgenden Server mit dem Wert '30':
   - Anwendungsserver
   - Ereignisserver
   - Datenserver
   - Verwaltungsserver

3. Inaktivieren Sie alle Linux-Firewalls.
4. Inaktivieren Sie SELinux (Security Enforcing Linux), indem Sie die Datei `/etc/selinux/config` bearbeiten und `SELINUX` in `disabled` ändern. Führen Sie nach der Änderung der Konfiguration einen Warmstart des Servers durch.
5. Stellen Sie sicher, dass alle Server dieselben vom Betriebssystem Linux angegebenen Uhrzeit- und Datumseinstellungen haben. Es kann ein Zeitsynchronisationsservice verwendet werden.
6. Aktivieren Sie den `sshd`-Service auf jedem Server, indem Sie den Befehl **/etc/init.d/sshd start** ausführen. Der Service muss über eine Rootanmeldung mit Kennwortauthentifizierung aktiviert werden. Für eine Verwendung während des Installationsprozesses muss der TCP/IP-Port 22 in dem Betriebssystem als verfügbarer SSH-Zugriffsport konfiguriert werden. Die TCP/IP-Portnummer für Plattformsteuerungstool SSH-Zugriff wird in der Datei mit den Topologieeigenschaften angegeben. Nur das Plattformsteuerungstool verwendet den konfigurierten Port.
7. Installieren Sie die Linux-Pakete in Tabelle 5 mithilfe des Befehls **yum install** *Paketname* auf jedem Server. Diese Pakete sind von Red Hat verfügbar.

Tabelle 5. Erforderliche und optionale Linux-Pakete für IBM Intelligent Operations Center-Zielserver

Paket	Anwendungsserver	Datenserver	Ereignisserver	Verwaltungsserver
`compat-libstdc++-33-3*`	erforderlich	erforderlich	erforderlich	erforderlich
`libXp-1.0.0-8*`	erforderlich	optional	erforderlich	erforderlich
`libXmu-1*`	erforderlich	optional	erforderlich	erforderlich
`libXtst-1*`	erforderlich	optional	erforderlich	erforderlich
`pam-0*`	erforderlich	optional	optional	optional
`rpm-build-4*`	erforderlich	optional	optional	erforderlich
`libaio-0*`	erforderlich	erforderlich	optional	erforderlich
`libstdc++-4*`	erforderlich	erforderlich	erforderlich	erforderlich
`libXft-2*`	erforderlich	optional	optional	erforderlich
`compat-db-4*`	erforderlich	optional	optional	erforderlich

Tabelle 5. Erforderliche und optionale Linux-Pakete für IBM Intelligent Operations Center-Zielserver (Forts.)

Paket	Anwendungsserver	Datenserver	Ereignisserver	Verwaltungsserver
elfutils-libs-0*	erforderlich	optional	optional	erforderlich
elfutils-0*	erforderlich	optional	optional	erforderlich
libgcc-4*	erforderlich	optional	erforderlich	optional
compat-glibc-2*	erforderlich	optional	erforderlich	optional
openmotif22-2*	erforderlich	optional	erforderlich	optional
audit-libs-1*	erforderlich	optional	optional	optional
glibc-2*	erforderlich	optional	optional	optional
glibc-common-2*	erforderlich	optional	optional	optional
glibc-headers-2*	optional	erforderlich	optional	erforderlich
glibc-devel-2*	optional	erforderlich	optional	erforderlich
compat-gcc*	optional	erforderlich	optional	erforderlich
libXft-2*	optional	optional	erforderlich	optional
libXpm-3*	optional	optional	erforderlich	optional
xorg-x11-xauth*	optional	optional	erforderlich	optional
ksh-*	optional	optional	optional	erforderlich

Die folgenden Befehle können für die Installation der erforderlichen Pakete auf jedem Server verwendet werden. Wenn das Paket bereits installiert ist, wird es nicht erneut installiert.

Anwendungsserver

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* pam-0*
rpm-build-4* libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0*
elfutils-0* libgcc-4* compat-glibc-2* openmotif22-2* audit-libs-1* glibc-2*
glibc-common-2*
```

Datenserver

```
yum install compat-libstdc++-33-3* libaio-0* libstdc++-4* glibc-headers-2*
glibc-devel-2* compat-gcc*
```

Ereignisserver

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* libstdc++-4*
libgcc-4* compat-glibc-2* openmotif22-2* libXft-2* libXpm-3* xorg-x11-xauth*
```

Verwaltungsserver

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* rpm-build-4*
libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0* elfutils-0*
glibc-headers-2* glibc-devel-2* compat-gcc* ksh-*
```

8. Stellen Sie sicher, dass Java 1.6 auf keinem der folgenden Server installiert ist:
   - Installationsserver
   - Anwendungsserver
   - Ereignisserver
   - Datenserver
   - Verwaltungsserver

Zugehörige Konzepte:

„Softwarevoraussetzungen” auf Seite 15
Vor der Installation von IBM Intelligent Operations Center muss auf den Servern die entsprechende Software installiert sein.

„IBM Intelligent Operations Center Hardwarevoraussetzungen” auf Seite 14
Es sind fünf Server erforderlich, die Mindestvoraussetzungen entsprechen, um IBM Intelligent Operations Center zu installieren.

Zugehörige Tasks:

„IBM Intelligent Operations Center mithilfe des Installation Managers installieren” auf Seite 28
IBM Intelligent Operations Center kann mithilfe des bereitgestellten grafisch orientierten Installationsprogramms installiert werden.

Zugehörige Informationen:

http://www.redhat.com/

TCP/IP-Netz einrichten

Vor der Installation von IBM Intelligent Operations Center muss das TCP/IP-Netz zwischen den Servern ordnungsgemäß eingerichtet werden.

Alle Server, einschließlich dem Installationsserver, der von IBM Intelligent Operations Center verwendet wird, müssen mit einem kurzen Hostnamen und einem vollständig qualifizierten Hostnamen konfiguriert sein. Die Hostnamen müssen auf jedem Server in die korrekten IP-Adressen aufgelöst werden. Die Konfiguration kann mithilfe eines DNS-Servers oder durch Hinzufügen von Definitionen zu der Datei `/etc/hosts` vorgenommen werden.

Der vollständig qualifizierte Hostname für jeden Server muss über mindestens drei Komponenten verfügen. Beispielsweise `myhost.mydomain.com`, wenn die Domäne der Ausgangsebene eine standardmäßige Internetdomäne der höchsten Ebene ist.

Wichtig: Kurze Hostnamen und vollständig qualifizierte Hostnamen müssen in der korrekten Groß-/Kleinschreibung eingegeben werden. Zum Beispiel darf MyCompany.MyDomain.com nicht als mycompany.mydomain.com eingegeben werden.

IPv6-Netzbetrieb wird von IBM Intelligent Operations Center unterstützt, aber IPv4 muss ebenfalls installiert und konfiguriert werden. Es ist nicht nötig, IPv4-Adressen Servern zuzuweisen, aber die IPv4-Prüfschleifenadresse (`127.0.0.1`) muss aktiviert sein und der Hostname `localhost` muss zu `127.0.0.1` aufgelöst werden.

Konfigurationsänderungen werden in Tabelle 6 auf Seite 24 angezeigt. Dies sind Richtlinien für die Einrichtung von TCP/IP-Netzbetrieb auf dem IBM Intelligent Operations Center Installationsserver und auf den Zielservern durch Bearbeitung der Linux-Netzkonfigurationsdateien. Die Anmerkungen zur Konfiguration in Tabelle 6 auf Seite 24 sind nur Richtlinien. Jede Netzkonfiguration, die den vorangehend beschriebenen Anforderungen entspricht, sollte funktionieren.

Tabelle 6. Richtlinien für die Konfiguration von TCP/IP

Datei	Anmerkungen

`/etc/hosts`	Die Datei `hosts` löst TCP/IP-Namen in IP-Adressen auf. Wenn die Konfiguration nicht über einen DNS-Server verfügt, müssen alle Server und ihre IP-Adressen, kurzen Hostnamen und vollständig qualifizierten Namen in dieser Datei definiert sein. Lokale Prüfschleifenadressen und Hostnamen sind ebenfalls in dieser Datei definiert.
	
	Wenn ein DNS-Server verwendet wird, müssen Hosts, die vom DNS aufgelöst werden, nicht in dieser Datei enthalten sein.
	Wichtig: Wenn IPv4 verwendet wird, muss die lokale Prüfschleifenadresse `127.0.0.1` den Hostnamen `localhost` und `localhost.localdomain` zugeordnet sein.
	
	Es folgt eine Beispieldatei `/etc/hosts`, die IPv4-Adressen verwendet.
	`# local loopback definitions -- do not remove`
	`# or alter these!`
	`127.0.0.1 localhost.localdomain localhost`
	`# use the following if IPv6 is enabled in your`
	`# network definitions`
	`::1 localhost6.localdomain localhost6`
	
	`# installation server`
	`192.168.0.205 IOC15Install.IOC15.com IOC15Install`
	
	`# target runtime servers`
	`192.168.0.211 IOC15App.IOC15.com IOC15App`
	`192.168.0.212 IOC15Event.IOC15.com IOC15Event`
	`192.168.0.213 IOC15DB.IOC15.com IOC15DB`
	`192.168.0.214 IOC15Mgmt.IOC15.com IOC15Mgmt`
	
	Verwenden Sie die IPv6-Adressenschreibweise, um statische IPv6-Adressen zuzuordnen.
	
	Sowohl IPv6- als auch IPv4-Adressen können auf demselben Server definiert werden.

Tabelle 6. Richtlinien für die Konfiguration von TCP/IP (Forts.)

Datei	Anmerkungen
/etc/sysconfig/network-scripts/ifcfg-*Adaptername*	Die Datei ifcfg-*Adaptername* definiert die grundlegenden Netzeinstellungen für den angegebenen Netzadapter. Der Linux zugeordnete Name für den Netzadapter wird von *Adaptername* angegeben. Der Standardwert für *Adaptername* ist eth0, aber er kann für Ihre Umgebung anders lauten. Die folgenden Parameter sollten für IPv4-Netzbetrieb definiert sein. **IPADDR** Geben Sie die IPv4 IP-Adresse des Servers an, der konfiguriert wird. **NETMASK** Geben Sie die IPv4-Netzmaske des Servers an, der konfiguriert wird. **GATEWAY** Geben Sie die IPv4 IP-Adresse des Standardnetzes des Servers an, der konfiguriert wird. **BOOTPROTO** Geben Sie, wenn statische IP-Adressierung verwendet wird, none an. **NM_CONTROLLED** Geben Sie den Wert no an, um den Netzmanagementservice für Änderungen an der Datei ifcfg-*Adaptername* zu sperren. **ONBOOT** Geben Sie den Wert yes an, um den Adapter automatisch zu starten. **IPV6INIT** Geben Sie den Wert yes an, wenn der Adapter IPv6-Netzbetrieb verwenden soll. **IPV6ADDR** Geben Sie die IPv6 IP-Serveradresse an, wenn IPV6INIT=yes festgelegt ist. **IPV6_DEFAULTGW** Geben Sie die standardmäßige IP-Adresse des Gateways für das IPv6-Netz an, wenn IPV6INIT=yes festgelegt ist.
/etc/sysconfig/network	Die Datei network gibt allgemeine Parameter des Netzbetriebs an. Für IPv4-Netzbetrieb sollten die folgenden Parameter definiert werden: **NETWORKING** Geben Sie den Wert yes an, um IPv4-Netzbetrieb zu aktivieren. **NETWORKING_IPV6** Geben Sie den Wert yes an, wenn auch IPv6-Netzbetrieb gewünscht ist. **HOSTNAME** Geben Sie den kurzen Hostnamen des Servers an.

Tabelle 6. Richtlinien für die Konfiguration von TCP/IP (Forts.)

Datei	Anmerkungen

`/etc/resolv.conf`	Die Datei `resolv.conf` wird verwendet, um DNS-Server für das Netz sowie eine standardmäßige Suchdomäne zu definieren. Wenn keine DNS-Server verwendet werden, sollte diese Datei leer sein.
	
	Wenn ein DNS-Server verwendet wird, sollte die Datei `resolv.conf` die folgenden Zeilen enthalten:
	`search`
	`Domänenname`
	`nameserver` *`erster_DNS-Server`*
	`nameserver`
	`zweiter_DNS-Server`
	
	Beispiel:
	`search yourcompany.com`
	`nameserver 10.75.20.10`
	`nameserver 10.75.20.11`
	
	Der Wert `search` (Suchen) gibt die standardmäßige Suchdomäne an. Der erste Wert `nameserver` ist die IP-Adresse des DNS-Servers. Ein zweiter Wert `nameserver` kann verwendet werden, um einen sekundären DNS-Server anzugeben. Die zweite Spezifikation `nameserver` ist optional.

`/etc/modprobe.conf`	Die Datei `modprobe.conf` definiert Konfigurationsoptionen für in das System geladene Module.
	
	IPv6-Netzbetrieb erfordert möglicherweise, dass die folgenden Zeilen auskommentiert und mit dem Server ein Warmstart durchgeführt wird:
	`alias ipv6 off`
	`options ipv6 disable=1`

Bei ordnungsgemäßer Konfiguration muss jeder Server die folgenden Tests erfolgreich bestehen:

1. Der Befehl **`hostname -s`** gibt den für den Server definierten kurzen Hostnamen zurück.
2. Der Befehl **`hostname -f`** gibt den vollständig qualifizierten Domänen- und Hostnamen für den Server zurück.
3. Das Ergebnis eines **`ping`**- oder eines **`ping6`**-Befehls (für IPV6-Umgebungen) mit den kurzen Hostnamen für die einzelnen Server weist darauf hin, dass auf den Server zugegriffen werden kann.
4. Das Ergebnis eines **`ping`**- oder eines **`ping6`**-Befehls (für IPV6-Umgebungen) mit den vollständig qualifizierten Hostnamen für die einzelnen Server weist darauf hin, dass auf den Server zugegriffen werden kann.

Zugehörige Tasks:

„Server vorbereiten" auf Seite 19
Überprüfen Sie vor der Installation von IBM Intelligent Operations Center, ob die Voraussetzungen für die Konfiguration des Servers erfüllt sind. Mithilfe des Vorabprüfungstools wird sichergestellt, dass ein Großteil dieser Voraussetzungen berücksichtigt wurde.

„IPv6-Netzbetrieb startet nicht" auf Seite 349
Wenn der IPv6-Netzbetrieb auf einem Server nicht startet, sind möglicherweise Änderungen der Datei `/etc/modprobe.conf` erforderlich.

„Vorabprüfungstool ausführen" auf Seite 46
Überprüfen Sie durch Ausführung des Vorabprüfungstools vor dem Hochladen von Installationspaketen auf die Zielserver, dass die Zielserver bereit für die Installation sind.

Das Installationspaket in den Installationsserver kopieren

Kopieren Sie das Installationspaket von IBM Intelligent Operations Center in den Installationsserver, bevor Sie das Produkt installieren.

Vorbereitende Schritte

Stellen Sie vor dem Kopieren des Installationspakets in den Installationsserver sicher, dass alle Server ordnungsgemäß vorbereitet sind.

Vorgehensweise

1. Erstellen Sie auf dem Installationsserver ein Verzeichnis für die Installationsdateien, z. B. `/installHome`.
2. Notieren Sie sich den vollständigen Pfad zu dem erstellten Verzeichnis. Wenn z. B. für den Benutzer `ibmadmin` das erstellte Verzeichnis `installHome` ist, dann lautet der Pfad `/home/ibmadmin/installHome`. Dieser Verzeichnispfad wird in anderen Installationsanweisungen als *Installationsausgangsverzeichnis* bezeichnet.
3. Gehen Sie für jede physische DVD oder jedes ISO-Image, die oder das von Passport Advantage heruntergeladen wurde, wie folgt vor:
   a. Erstellen Sie ein Verzeichnis, um die DVD anzuhängen. Führen Sie z. B. den Befehl **mkdir /mnt/ba15** aus.
   b. Die DVD anhängen. Wenn Sie beispielsweise ein ISO-Image verwenden, führen Sie den Befehl **mount -o loop***ISO-Verzeichnis*/*ISO-Dateiname*/**mnt/ba15** aus. Dabei ist *ISO-Verzeichnis* die Position des ISO-Image, und *ISO-Dateiname* ist die ISO-Datei.
   c. Kopieren Sie die DVD-Inhalte in das in Schritt 1 erstellte Verzeichnis. Wenn Sie beispielsweise ein ISO-Image verwenden, führen Sie den Befehl **cp /mnt/ba15/*** *Installationsausgangsverzeichnis* aus.
   d. Die DVD abhängen. Wenn Sie beispielsweise ein ISO-Image verwenden, führen Sie den Befehl **umount /mnt/ba15** aus.
4. Wechseln Sie in das *Installationsausgangsverzeichnis*.
5. Führen Sie den Befehl **ba15_media_prep.sh combine** aus. Dieser Befehl muss ausgeführt werden, bevor Sie andere Installationsschritte durchführen.

   Anmerkung: Wenn Ihr Verzeichnis *install_home* ein anderes Verzeichnis ist als `/installMedia`, bearbeiten Sie die Datei `ba15_media_prep.sh` und ändern Sie den Wert `MEDIA_BASE` zu Ihrem dedizierten Verzeichnis *install_home*, bevor Sie das Script ausführen.
   Dieser Befehl kombiniert Dateien, die auf DVDs oder ISO-Images aufgeteilt sind.

Zugehörige Konzepte:

„Position der Installationsmedien” auf Seite 33
Mit dem IBM Installation Manager ist es dem Installationsverantwortlichen möglich, anzugeben, wo die Installationspakete während der Installation von IBM Intelligent Operations Center positioniert sind.

Zugehörige Tasks:

„IBM Intelligent Operations Center mithilfe des Installation Managers installieren”
IBM Intelligent Operations Center kann mithilfe des bereitgestellten grafisch orientierten Installationsprogramms installiert werden.

„Die Java-Laufzeitumgebung installieren”
Die Java 6 Runtime-Umgebung muss auf dem Installationsserver installiert sein, bevor IBM Intelligent Operations Center installiert wird.

Die Java-Laufzeitumgebung installieren

Die Java 6 Runtime-Umgebung muss auf dem Installationsserver installiert sein, bevor IBM Intelligent Operations Center installiert wird.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

1. Melden Sie sich als `root` an, oder wechseln Sie zum Root-Account, indem Sie den Befehl **`su -`** ausführen.
2. Wechseln Sie in das Verzeichnis, in das die Installationsdateien von IBM Intelligent Operations Center kopiert wurden.
3. Führen Sie den Befehl **`yum --nogpgcheck install`** *Installationsmedien*`/ibm-java-x86_64-jre-6.0-10.1.x86_64.rpm` aus.
4. Führen Sie den Befehl **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`** aus.
5. Überprüfen Sie die Java-Umgebung, indem Sie den Befehl **`echo $JAVA_HOME`** ausführen und bestätigen, dass `/opt/ibm/java-x86_64-60/jre` zurückgegeben wurde.

Zugehörige Tasks:

„Das Installationspaket in den Installationsserver kopieren” auf Seite 27
Kopieren Sie das Installationspaket von IBM Intelligent Operations Center in den Installationsserver, bevor Sie das Produkt installieren.

„Das Plattformsteuerungstool konfigurieren” auf Seite 64
Nach der Installation von IBM Intelligent Operations Center müssen Sie, sofern Sie eine andere Java™ JRE installiert haben als die mit IBM Intelligent Operations Center bereitgestellte, die JRE-Position definieren, die vom Plattformsteuerungstool verwendet wird.

„IBM Intelligent Operations Center mithilfe des Installation Managers installieren”
IBM Intelligent Operations Center kann mithilfe des bereitgestellten grafisch orientierten Installationsprogramms installiert werden.

IBM Intelligent Operations Center mithilfe des Installation Managers installieren

IBM Intelligent Operations Center kann mithilfe des bereitgestellten grafisch orientierten Installationsprogramms installiert werden.

Vorbereitende Schritte

Das Produktpaket muss in den Installationsserver im Verzeichnis *Installationsausgangsverzeichnis* kopiert werden, bevor diese Schritte durchgeführt werden.

Informationen zu diesem Vorgang

Während der Installation wird ein Statusanzeigefeld angezeigt. Allerdings zeigt das Statusanzeigefeld nicht die genaue verbleibende Dauer der Installation an, da Installationstasks über Fernzugriff auf Zielservern durchgeführt werden. In der Datei „Installationskomponenten" auf Seite 32 ist die geschätzte Installationsdauer für jede Komponente angegeben.

Wenn Sie die Installation an einem beliebigen Punkt abbrechen möchten, klicken Sie auf **Abbrechen** in der Benutzeroberfläche von IBM Installation Manager.

Wichtig: Führen Sie nach der erfolgreichen Installation der ersten Komponente nicht den Befehl **launchpad.sh** aus. Sie erhalten nicht die Option, Ihre Installation zu ändern. Verwenden Sie stattdessen den Befehl **/opt/IBM/InstallationManager/eclipse/IBMIM**, um das Installationsprogramm, wie in Schritt 24 auf Seite 30 beschrieben, neu zu starten.

Vorgehensweise

1. Führen Sie den Befehl **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** aus.
2. Extrahieren Sie die Datei `BA_1.5_GUI_Installer_Lite_Launchpad.zip` in das *Installationsausgangsverzeichnis*.
3. Starten Sie den Installationsassistenten durch Ausführen des Befehls *Installationsausgangsverzeichnis*/**launchpad.sh**.
4. Installieren Sie IBM Installation Manager.
   a. Klicken Sie auf **IBM Installation Manager installieren**.
   b. Klicken Sie auf **Weiter**.
   c. Lesen Sie die Lizenzinformationen.
   d. Wenn Sie den Lizenzbedingungen zustimmen, wählen Sie `Ich akzeptiere die Bedingungen der Lizenzvereinbarung` aus und klicken Sie auf **Weiter**. Die Installation wird fortgesetzt.
   e. Wenn Sie den Lizenzbedingungen nicht zustimmen, wählen Sie `Ich akzeptiere die Bedingungen der Lizenzvereinbarung nicht` aus und klicken Sie auf **Weiter**. Die Installation wird beendet.
   f. Wählen Sie aus, wo IBM Installation Manager installiert werden soll.
   g. Klicken Sie auf **Weiter**.
   h. Klicken Sie auf **Installieren**.
   i. Starten Sie den IBM Installation Manager neu.

   IBM Installation Manager wurde installiert.
5. Nachdem der IBM Installation Manager installiert wurde, muss IBM Installation Manager geschlossen und neu gestartet werden. Durch Starten des IBM Installation Manager vom Launchpad aus wird die Topologiedatei für IBM Intelligent Operations Center berücksichtigt.
6. Klicken Sie auf **IBM Intelligent Operations Center installieren**.
7. Wählen Sie das Paket `IBM Intelligent Operations Center - Version 1.5` aus.
8. Klicken Sie auf **Weiter**.
9. Lesen Sie die Lizenzinformationen.
   a. Wenn Sie den Lizenzbedingungen zustimmen, wählen Sie `Ich akzeptiere die Bedingungen der Lizenzvereinbarung` aus und klicken Sie auf **Weiter**. Die Installation wird fortgesetzt.
   b. Wenn Sie den Lizenzbedingungen nicht zustimmen, wählen Sie `Ich akzeptiere die Bedingungen der Lizenzvereinbarung nicht` aus und klicken Sie auf **Weiter**. Die Installation wird beendet.

10. Legen Sie das Verzeichnis für gemeinsam genutzte Ressourcen für diese Installation fest. Dieses Verzeichnis wird immer verwendet, wenn Sie den IBM Installation Manager verwenden, um Produkte mithilfe des Installationsserver zu installieren. Stellen Sie sicher, dass Sie das Laufwerk mit dem meisten verfügbaren Speicherplatz auf dem Server festlegen.
11. Klicken Sie auf **Weiter**.
12. Erstellen Sie eine neue Paketgruppe, indem Sie Neue Paketgruppe erstellen auswählen. Wählen Sie IBM Intelligent Operations Center aus.
13. Geben Sie den Namen des Installationsverzeichnisses an. Das Installationsverzeichnis wird erstellt. Das Installationsprogramm erstellt bei Bedarf unterhalb dieses Verzeichnisses Unterverzeichnisse.
14. Wählen Sie bei Architekturauswahl 64-Bit aus.
15. Klicken Sie auf **Weiter**.
16. Heben Sie die Auswahl aller Optionen auf.
17. Wählen Sie **Topologie konfigurieren** aus.
18. Klicken Sie auf **Weiter**.
19. Geben Sie die Konfigurationsoptionen ein. Notieren Sie sich alle definierten Kennwörter.
20. Klicken Sie auf **Weiter**.
21. Überprüfen Sie die Installationsoptionen und klicken Sie auf **Weiter**, um die Installation zu starten.
22. Nachdem die Installation abgeschlossen ist, schließen Sie IBM Installation Manager und das Launchpad. Schließen Sie das Terminalfenster nicht, wenn das Launchpad in Schritt 3 auf Seite 29 gestartet wurde, denn es ist auf die Umgebung JAVA_HOME eingestellt. Wenn das Terminalfenster geschlossen ist, muss JAVA_HOME erneut exportiert werden, bevor der Vorgang fortgesetzt werden kann.
23. Wenn der für das Topologiekennwort eingegebene Wert mehr als 15 Zeichen lang ist, befolgen die die folgenden Schritte, um ein Kennwort für ITM.ADMIN.USER.PWD zu definieren, das höchstens 15 Zeichen lang ist.
    a. Bearbeiten Sie auf dem Installationsserver die Datei *Installationsausgangsverzeichnis*/ioc/topology/iop_lite_topo.properties, wobei *Installationsausgangsverzeichnis* das Verzeichnis ist, in das das Installationspaket von IBM Intelligent Operations Center kopiert wurde.
    b. Ändern Sie den für das Kennwort ITM.ADMIN.USER.PWD definierten Wert, sodass er nicht mehr als 15 Zeichen umfasst. Dieses Kennwort wird anstelle des Topologiekennwortes für die Anmeldung des Benutzers sysadmin verwendet.
    c. Speichern Sie die Änderungen.
24. Starten Sie den IBM Installation Manager, indem Sie den Befehl **/opt/IBM/InstallationManager/eclipse/IBMIM** ausführen.
25. Klicken Sie auf **Ändern** > **Weiter**.
26. Wählen Sie **Zielserver vorbereiten** aus.
27. Klicken Sie auf **Weiter** > **Ändern**.
28. Sollten Fehler auftreten, überprüfen Sie die Protokolldateien im Verzeichnis /var/ibm/InstallationManager/logs/native. Die Namen von Protokolldateien beginnen mit einer Zeitmarke, die verwendet werden kann, um das Protokoll zu erkennen, wenn das Installationstool ausgeführt wurde.
29. Korrigieren Sie alle in den Protokollen gefundenen Fehlernachrichten oder Warnungen, die Ihr System betreffen, und beenden Sie die Installation, bevor Sie die nächste Komponente installieren. Manche Warnungen und Fehlernachrichten können ignoriert werden. Das gilt z. B. für Warnungen über IPv6, wenn Sie IPv6 nicht aktiviert haben oder wenn Ihre Konfiguration nicht mit einem Domain Name Service (DNS) verbunden ist.
30. Kehren Sie, nachdem Sie alle Fehler korrigiert haben, zu Schritt 25 zurück. Sie verfügen über die Option, Systemprüffehler zu ignorieren. Wählen Sie die nächste Komponente in der Liste in Schritt 26 aus. Setzen Sie den Prozess fort, bis Cyber Hygiene installiert werden soll.

Wichtig: Schalten Sie die Server zwischen den Installationsphasen nicht herunter. Das Herunterfahren von Servern zwischen Installationsphasen wurde nicht getestet und kann zu unvorhersehbaren Ergebnissen führen.

Cyber Hygiene greift auf bewährte Konfigurationen zurück, um zusätzliche Sicherheit für das IBM Intelligent Operations Center-System bereitzustellen. Schließen Sie die Konfiguration nach der Installation zuerst ab, bevor Sie Cyber Hygiene installieren. Wenn die Konfiguration nach der Installation beendet ist, kehren Sie zu Schritt 24 auf Seite 30 zurück, installieren Sie Cyber Hygiene, und führen Sie es aus. Komponenten, die bei der vorangegangenen Ausführung von IBM Installation Manager erfolgreich installiert wurden, werden überprüft. Diese Komponenten dürfen nicht inaktiviert werden, da sie ansonsten deinstalliert werden, wenn IBM Installation Manager erneut ausgeführt wird.

Wenn die Ausführung in einer virtualisierten Umgebung stattfindet, erstellen Sie vom Speicher aller Server nach einem erfolgreich beendeten Installationsschritt und vor der Installation der nächsten Komponente eine Momentaufnahme. Diese Momentaufnahme kann verwendet werden, um die Installation nach einem erfolgreich verlaufenen Installationsschritt neu zu starten, falls ein Fehler auftritt.

Hängen Sie alle Dateisysteme, die nicht bezüglich ihrer Sicherheit beurteilt werden sollen, ab, um die Zeit, die Cyber Hygiene für das Ausführen von Scans und Korrekturen benötigt, zu reduzieren. Z. B. können die Verzeichnisse *Installationsmedien* auf jedem Server nach Abschluss aller Installationsschritte gelöscht werden. Diese Verzeichnisse können vor dem Ausführen von Cyber Hygiene gelöscht oder abgehängt werden.

Anmerkung: Cyber Hygiene wird innerhalb desselben Schrittes installiert und ausgeführt.

Das Ausführen von Cyber Hygiene sollte der letzte Schritt sein, bevor Sie Ihr System in Produktionsstatus versetzen oder wenn Ihr System gute Sicherheitsverfahren verwenden muss. Alle Anwendungen und Lösungen sollten installiert und konfiguriert sein, bevor Cyber Hygiene ausgeführt wird, damit das letzte System gescannt werden kann und Korrekturen ausgeführt werden können.

Von Cyber Hygiene vorgenommene Änderungen am System können zu Problemen mit anderen Anwendungen und Lösungen führen. Beispielsweise haben andere Anwendungen und Lösung möglicherweise Anforderungen an die Linux-Umgebung, die nicht mit den guten Sicherheitsverfahren übereinstimmen. Für die Installation oder Ausführung einer Anwendung oder Lösung ist es möglicherweise erforderlich, dass die Anmeldung an das System als `Root`benutzer erfolgt. In diesem Fall müssen manche der Änderungen von Cyber Hygiene temporär oder dauerhaft geändert werden oder vom Anbieter der Anwendung oder Lösung muss eine andere Lösungsmöglichkeit gefunden werden.

Sind Änderungen von Cyber Hygiene einmal vorgenommen, gibt es keine automatisierte Methode, sie zu ändern. Alle Änderungen müssen durch manuelle Aktualisierungen des Betriebssystems Linux oder durch Änderung der Datei- oder Verzeichnisberechtigungen erfolgen.

Zugehörige Konzepte:

„Installationsservices aus dem Produktionssystem entfernen" auf Seite 72
Nach der Installation von IBM Intelligent Operations Center können die Installationsservices von den Produktionssystemservern entfernt werden. Es wird empfohlen, dass der Installationsserver beibehalten wird, da möglicherweise einige der Services für Verwaltungsaktivitäten benötigt werden.

„Konfiguration nach der Installation von IBM Intelligent Operations Center" auf Seite 56
Nach der schrittweise oder mithilfe des Installation Managers durchgeführten Installation der IBM Intelligent Operations Center-Architektur sind mehrere Schritte der Konfiguration nach der Installation erforderlich, um die Installation abzuschließen.

„Übersicht über Cyber Hygiene" auf Seite 87
Das IBM Intelligent Operations Center-Feature Cyber Hygiene stellt Services bereit, um gegen potenzielle Sicherheitsrisiken im installierten System vorzugehen.

Zugehörige Tasks:

„Server vorbereiten" auf Seite 19
Überprüfen Sie vor der Installation von IBM Intelligent Operations Center, ob die Voraussetzungen für die Konfiguration des Servers erfüllt sind. Mithilfe des Vorabprüfungstools wird sichergestellt, dass ein Großteil dieser Voraussetzungen berücksichtigt wurde.

„Installation überprüfen" auf Seite 55
Überprüfen Sie nach der Installation von IBM Intelligent Operations Center dass das Produkt ordnungsgemäß installiert wurde.

„Das Installationspaket in den Installationsserver kopieren" auf Seite 27
Kopieren Sie das Installationspaket von IBM Intelligent Operations Center in den Installationsserver, bevor Sie das Produkt installieren.

„Die Java-Laufzeitumgebung installieren" auf Seite 28
Die Java 6 Runtime-Umgebung muss auf dem Installationsserver installiert sein, bevor IBM Intelligent Operations Center installiert wird.

Installationskomponenten

Die Installation von IBM Intelligent Operations Center umfasst sieben Komponenten.

Tabelle 7. IBM Intelligent Operations Center-Installationskomponenten

Komponente	Geschätzte Installationszeit	Was wird installiert?
Installation vorbereiten	Vorabprüfung: 10 Minuten Hochladen: 2 Stunden	Es wird geprüft, ob die Serverumgebung die Mindestvoraussetzungen erfüllt, und die für die Installation erforderlichen Dateien werden auf die Zielserver kopiert.
Umgebung vorbereiten	10 Minuten	Aktualisiert nach Bedarf die `/etc/sudoers` und `~/.ssh/known_hosts`-Dateien für IBM Intelligent Operations Center
Plattform installieren und konfigurieren	Phase 1: 12 Stunden Phase 2: 3 Stunden	Die erforderliche Plattform wird auf den Zielservern installiert. Die Installation wird in zwei Phasen ausgeführt.
Plattformsteuerungstool	10 Minuten	Tools, die zum Starten, Stoppen und Abfragen des Status der IBM Intelligent Operations Center-Server erforderlich sind, werden auf dem Management-Server installiert.
Platform Systemprüfung	15 Minuten	Tools zum Bestimmen, ob Schlüsselfunktionen der Plattform auf dem Anwendungsserver installiert sind.
Anwendungsserver	3 Stunden	Die e IBM Intelligent Operations Center-Anwendung wird auf den Zielservern installiert.

Tabelle 7. IBM Intelligent Operations Center-Installationskomponenten (Forts.)

Komponente	Geschätzte Installationszeit	Was wird installiert?
Cyber Hygiene	Bis zu 1,5 Stunden	Funktionen zur Risikominderung und Korrektur bekannter Cybersicherheitsrisiken werden auf den Zielservern installiert. Die Verarbeitungszeit hängt von der Geschwindigkeit der Hardware ab und davon, ob sich zusätzliche, unnötige Dateien auf den Zielservern befinden.

Konfigurationsoptionen

Der IBM Installation Manager erlaubt dem Installationsprogramm die Angabe von Konfigurationsoptionen während der Installation des IBM Intelligent Operations Center.

Topologiekennwort

Der IBM Installation Manager erlaubt dem Installationsprogramm die Angabe der Kennwörter, die mit dem IBM Intelligent Operations Center verwendet werden.

Das Installationsprogramm kann die in Tabelle 8 angezeigten Kennwörter angeben.

Tabelle 8. IBM Intelligent Operations Center-Kennwörter

Kennwort	Beschreibung
Topologiekennwort	Das Topologiekennwort ist das Kennwort, das für alle vom IBM Intelligent Operations Center-Installationsprogramm erstellten Konten verwendet wird, mit Ausnahme der Kennwörter, die während des Installationsprozesses speziell angefordert werden, und des Kennworts `iicsystemuser`, das als `passw0rd` definiert ist und nicht geändert werden kann. Das Topologiekennwort schützt auch den geheimen Schlüssel, der vom Befehl **`createSecretKey`** erstellt wird. Das Kennwort für ein Konto darf maximal 15 Zeichen aufweisen. Wenn das Topologiekennwort länger als 15 Zeichen ist, müssen spezielle Konfigurationsschritte durchgeführt werden, um das Kennwort für dieses Konto neu zu definieren.
Administratorkennwort	Das Administratorkennwort, das für den Linux-Benutzer `ibmadmin` festgelegt wurde. Dieser Benutzer wird vom Plattformsteuerungstool für die Verwaltung der Zielserverkomponenten verwendet.
Seedwert für die Verschlüsselung	Der Seedwert für die Verschlüsselung wird verwendet, um Benutzerkennwörter und andere sensible Daten in der Datenbank zu verschlüsseln. Der Seedwert für die Verschlüsselung muss ein Wert mit 12 bis 1016 druckbaren ASCII-Zeichen sein. Eine stark typisierte Zeichenfolge sollte verwendet werden. Beispiel: Eine lange Zeichenfolge, die aus Buchstaben in Groß-/Kleinschreibung, Zahlen und Sonderzeichen ohne allgemeine Wörter oder Wortfolgen besteht.
Saltwert für die Verschlüsselung	Der Saltwert für die Verschlüsselung wird verwendet, um Benutzerkennwörter und andere sensible Daten in der Datenbank zu verschlüsseln. Der Saltwert für die Verschlüsselung muss ein Wert mit 12 druckbaren ASCII-Zeichen zwischen den Codepunkten 33 und 126 sein.

Position der Installationsmedien

Mit dem IBM Installation Manager ist es dem Installationsverantwortlichen möglich, anzugeben, wo die Installationspakete während der Installation von IBM Intelligent Operations Center positioniert sind.

Der Installationsverantwortliche kann die in Tabelle 9 auf Seite 34 aufgeführten Installationsverzeichnisse angeben.

Tabelle 9. Installationsverzeichnisse von IBM Intelligent Operations Center

Verzeichnis	Beschreibung	Empfohlener Wert
Lokales Basisverzeichnis für Images	Der Name des Verzeichnisses auf dem Installationsserver, das die Installationsdateien für IBM Intelligent Operations Center enthält. In dieses Verzeichnis werden vor Ausführung des Installationstools die Installationsmediendateien kopiert. In sonstigen Installationsanweisungen wird dieses Verzeichnis als *Installationsmedien* bezeichnet.	`/installMedia`
Lokales temporäres Verzeichnis für Images	Das Verzeichnis auf dem Installationsserver, in dem während der Installation temporäre Dateien gespeichert werden.	`/installMedia`
Lokales Sicherungsverzeichnis	Dieses Verzeichnis ist nur für interne Zwecke bestimmt.	`/tmp/loc/backup`
Fernes Imageverzeichnis	Das Verzeichnis auf den Zielservern, in das die Pakete kopiert werden, die auf den jeweiligen Servern installiert werden sollen.	`/installMedia/loc/image`
Fernes Scriptverzeichnis	Das Verzeichnis auf den Zielservern, in das die Installationsscripts kopiert werden, die auf den jeweiligen Servern ausgeführt werden sollen.	`/installMedia/loc/script`

Zugehörige Tasks:

„Das Installationspaket in den Installationsserver kopieren" auf Seite 27
Kopieren Sie das Installationspaket von IBM Intelligent Operations Center in den Installationsserver, bevor Sie das Produkt installieren.

Datenserver-Standort

Der IBM Installation Manager erlaubt dem Installationsprogramm die Definition der Verbindung zum Datenserver während der Installation des IBM Intelligent Operations Center.

Das Installationsprogramm kann die Datenserver-Verbindungsoptionen angeben, die in Tabelle 10 angegeben sind.

Tabelle 10. IBM Intelligent Operations Center Datenserver-Verbindungsinformationen

Option	Beschreibung	Empfohlener Wert
Datenserver-Hostname	Der vollständig qualifizierte Hostname für den Server.	Keiner. Der Wert hängt von der Installation ab.
Datenserver-Benutzer	Das Linux-Benutzerkonto, das während des Installationsprozesses verwendet wird.	`root`
Datenserver-Kennwort	Das Kennwort für das Konto, das in **Data Server-Benutzer** angegeben ist.	Keiner. Der Wert hängt von der Installation ab.

Um die Verbindung zum Server zu testen, klicken Sie auf **Verbindung testen**.

Anwendungsserver-Standort

Der IBM Installation Manager erlaubt dem Installationsprogramm die Definition der Verbindung zum Anwendungsserver während der Installation des IBM Intelligent Operations Center.

Das Installationsprogramm kann die Anwendungsserver-Verbindungsoptionen angeben, die in Tabelle 11 auf Seite 35 angegeben sind.

Tabelle 11. IBM Intelligent Operations Center Anwendungsserver-Verbindungsinformationen

Option	Beschreibung	Empfohlener Wert
Anwendungsserver-Hostname	Der vollständig qualifizierte Hostname für den Server.	Keiner. Der Wert hängt von der Installation ab.
Anwendungsserver-Benutzer	Das Linux-Benutzerkonto, das während des Installationsprozesses verwendet wird.	`root`
Anwendungsserver-Kennwort	Das Kennwort für das Konto, das unter **Anwendungsserverbenutzer** angegeben ist.	Keiner. Der Wert hängt von der Installation ab.

Um die Verbindung zum Server zu testen, klicken Sie auf **Verbindung testen**.

Ereignisserver-Standort

Der IBM Installation Manager erlaubt dem Installationsprogramm die Definition der Verbindung zum Ereignisserver während der Installation des IBM Intelligent Operations Center.

Das Installationsprogramm kann die Ereignisserver-Verbindungsoptionen angeben, die in Tabelle 12 angegeben sind.

Tabelle 12. IBM Intelligent Operations Center Ereignisserver-Verbindungsinformationen

Option	Beschreibung	Empfohlener Wert
Ereignisserver-Hostname	Der vollständig qualifizierte Hostname für den Server.	Keiner. Der Wert hängt von der Installation ab.
Ereignisserver-Benutzer	Das Linux-Benutzerkonto, das während des Installationsprozesses verwendet wird.	`root`
Ereignisserver-Kennwort	Das Kennwort für das Konto, das in **Ereignisserverbenutzer** angegeben ist.	Keiner. Der Wert hängt von der Installation ab.

Um die Verbindung zum Server zu testen, klicken Sie auf **Verbindung testen**.

Verwaltungsserver-Standort

Der IBM Installation Manager erlaubt dem Installationsprogramm die Definition der Verbindung zum Verwaltungsserver während der Installation des IBM Intelligent Operations Center.

Das Installationsprogramm kann die Verwaltungsserver-Verbindungsoptionen angeben, die in Tabelle 13 angegeben sind.

Tabelle 13. IBM Intelligent Operations Center Verwaltungsserver-Verbindungsinformationen

Option	Beschreibung	Empfohlener Wert
Verwaltungsserver-Hostname	Der vollständig qualifizierte Hostname für den Server.	Keiner. Der Wert hängt von der Installation ab.
Verwaltungsserver-Benutzer	Das Linux-Benutzerkonto, das während des Installationsprozesses verwendet wird.	`root`
Verwaltungsserver-Kennwort	Das Kennwort für das Konto, das in **Management-Serverbenutzer** angegeben ist.	Keiner. Der Wert hängt von der Installation ab.

Um die Verbindung zum Server zu testen, klicken Sie auf **Verbindung testen**.

Konfiguration von Cyber Hygiene

Der IBM Installation Manager erlaubt dem Installationsprogramm die Angabe der erforderlichen Optionen für Cyber Hygiene während der Installation des IBM Intelligent Operations Center.

Das Installationsprogramm kann die in Tabelle 14 angezeigten Optionen für Cyber Hygiene angeben.

Tabelle 14. Optionen für Cyber Hygiene für IBM Intelligent Operations Center

Option	Beschreibung	Empfohlener Wert
GRUB-Kennwort	Das Kennwort für das Bootladeprogramm für das System. Dieses Kennwort wird für alle Zielserver verwendet.	Ein Kennwort, das vom Kunden angegeben wird und der Kennwortrichtlinie der Organisation des Kunden entspricht.
Ferne Rootanmeldung inaktivieren	Definiert, ob der Fernzugriff für den Rootbenutzer auf allen Zielservern inaktiviert ist.	Ein Kontrollkästchen mit der ausgewählten Option wird angezeigt. Die Auswahl der Option kann nicht aufgehoben werden. Die ferne Rootanmeldung muss inaktiviert sein. Die Option wird angezeigt, sodass das Installationsprogramm versteht, dass die ferne Rootanmeldung inaktiviert ist. Bei dieser Konfiguration ist die Anmeldung als `root` von der Konsole aktiviert und der Benutzer kann zum `root`-Benutzer mit dem Befehl **`su`** wechseln, wenn er beim Server angemeldet ist.

Installation mithilfe von Installation Manager neu starten

Wenn die Installation fehlschlägt, kann sie neu gestartet werden.

Informationen zu diesem Vorgang

Wenn die Installation fehlschlägt, macht das Installationstool Änderungen rückgängig, die während der Sitzung vorgenommen wurden. Wenn mehrere Installationskomponenten ausgewählt wurden, werden alle ausgewählten Schritte rückgängig gemacht, auch wenn manche der Schritte erfolgreich abgeschlossen wurden.

Gehen Sie wie folgt vor, um eine fehlgeschlagene Installation neu zu starten.

Vorgehensweise

1. Klicken Sie auf **Anwendungen** > **IBM Installation Manager** > **IBM Installation Manager**.
2. Wenn keine Komponente erfolgreich installiert wurde, wählen Sie **Neu** aus, um die Installation von Anfang an neu zu starten.
3. Wenn eine oder mehrere Komponenten erfolgreich installiert wurden, wählen Sie **Ändern** aus, um vorhandene Installationsänderungen beizubehalten. Wählen Sie die Komponente oder die Komponenten aus, die installiert werden sollen.

   Anmerkung: Es wird empfohlen, das Installationsprogramm zu verwenden, um Komponenten nacheinander zu installieren. Dadurch wird das Rückgängigmachen von erfolgreich installierten Komponenten begrenzt, wenn nachfolgende Komponenteninstallationen fehlschlagen.

IBM Intelligent Operations Center schrittweise installieren

IBM Intelligent Operations Center kann mithilfe von schrittweisen Installationsschritten und Scripts installiert werden.

Installationspaket vorbereiten

Vor der Ausführung der Installationsscripts muss das Installationspaket entpackt und vorbereitet werden.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

1. Kopieren Sie das Installationspaket nach *Installationsausgangsverzeichnis*.
2. Extrahieren Sie das Installationspaket.
3. Extrahieren Sie BA_1.5_GUI_Installer_Lite_Launchpad.zip in das *Installationsausgangsverzeichnis*.
4. Wechseln Sie in das Verzeichnis *Installationsausgangsverzeichnis*/repository/native.
5. Extrahieren Sie com.ibm.iop.ba.lite_1.5.0.9.zip in das *Installationsausgangsverzeichnis*.
6. Extrahieren Sie com.ibm.iop.cat.lite_1.5.0.9.zip in das *Installationsausgangsverzeichnis*.
7. Extrahieren Sie com.ibm.iop.isp.lite_1.5.0.zip in das Verzeichnis *Installationsausgangsverzeichnis*/isp/.
8. Extrahieren Sie com.ibm.iop.cyber.hygiene.install.lite_1.5.0.zip in das Verzeichnis *Installationsausgangsverzeichnis*/ch.
9. Führen Sie den Befehl **cp ../ files/com.ibm.iop.cyber.hygiene.scripts.lite_1.5.0.zip [install-home]/ch/install** aus.
10. Extrahieren Sie com.ibm.iop.ioc.solution.lite_1.5.0.20120807.1518.zip in das Verzeichnis *Installationsausgangsverzeichnis*/ioc/spec.
11. Extrahieren Sie com.ibm.iop.ioc.topology.lite_1.5.0.20120807.1518.zip in das Verzeichnis *Installationsausgangsverzeichnis*/ioc/topology.
12. Führen Sie den Befehl **find** *Installationsausgangsverzeichnis* **-name *.sh -exec chmod +x {} \;** aus.
13. Führen Sie den Befehl **find** *Installationsausgangsverzeichnis* **-name *.sh -exec dos2unix {} \;** aus.

Installationsscripts überprüfen

Ein Befehl kann so ausgeführt werden, dass er Dokumentation über das Installationsprogramm anzeigt. Dies zeigt außerdem, dass das Installationspaket aktiv ist.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

1. Melden Sie sich als root an oder wechseln Sie zum Root-Account, indem Sie den Befehl **su -** ausführen.
2. Führen Sie den Befehl **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** aus.
3. Führen Sie den Befehl *install_home***/ioc/bin/ba.sh** aus. Installationsdokumentation wird angezeigt.

Installationseigenschaften anpassen

Die Datei mit den Installationseigenschaften und die Dateien mit den Topologieeigenschaften stellen Definitionen bereit, die von den Installationsscripts benötigt werden.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

Optional: Bearbeiten Sie die Datei *install_home*/ioc/resource/custom.properties und ändern Sie bei Bedarf die folgenden Eigenschaftswerte. Eigenschaftswerte in der Datei, die nicht in Tabelle 15 aufgelistet sind, sollten nicht geändert werden.

Tabelle 15. Installationseigenschaften von IBM Intelligent Operations Center

Eigenschaft	Beschreibung	Standardwert
image.basedir.local	Der Name des Verzeichnisses auf dem Installationsserver, das die Installationsdateien für IBM Intelligent Operations Center enthält. In dieses Verzeichnis werden vor Ausführung des Installationstools die Installationsmediendateien kopiert. In sonstigen Installationsanweisungen wird dieses Verzeichnis als *Installationsmedien* bezeichnet.	/installMedia
image.tempdir.local	Das Verzeichnis auf dem Installationsserver, in dem während der Installation temporäre Dateien gespeichert werden.	/installMedia
backup.local	Dieses Verzeichnis ist nur für interne Zwecke bestimmt.	/tmp/loc/backup
Unix.image.basedir.remote	Das Verzeichnis auf den Zielservern, in das die Pakete kopiert werden, die auf den jeweiligen Servern installiert werden sollen.	/installMedia/loc/image
Unix.script.basedir.remote	Das Verzeichnis auf den Zielservern, in das die Installationsscripts kopiert werden, die auf den jeweiligen Servern ausgeführt werden sollen.	/installMedia/loc/script
connection.timeout	Dauer (in Millisekunden), für die auf eine Verbindung zu den Zielservern gewartet wird, bevor der Versuch abgebrochen wird	120000
waiting.time	Dauer (in Millisekunden), für die gewartet wird, bevor nach einer fehlgeschlagenen Verbindung ein Neuversuch unternommen wird	120000
retry.count	Zahl der Neuversuche einer fehlgeschlagenen Verbindung, bevor die Installation fehlschlägt	6

Wenn keine Änderung vorgenommen wird, werden die Standardwerte verwendet.

Zugehörige Konzepte:

„Kennwortinformationen” auf Seite 41

Kennwörter für mehrere Benutzer-IDs, die in der IBM Intelligent Operations Center-Lösung verwendet werden, sind in der Datei mit den Topologieeigenschaften definiert. Aus Sicherheitsgründen sollten die mit IBM Intelligent Operations Center ausgelieferten Standardkennwörter geändert werden.

Installation mit Topologiedateien

IBM Intelligent Operations Center wird mithilfe einer Topologiedatei installiert. Die Topologiedatei ist eine XML-Datei, die die Parameter und Werte definiert, die beim Einsatz von IBM Intelligent Operations Center über verschiedene Server verwendet werden. Darüber hinaus definiert die Topologiedatei die zur Implementierung von Komponenten verwendete Sequenz.

Die Bearbeitung der Topologiedatei mit einem Texteditor kann zu Fehlern führen. Deshalb sind alle durch den Benutzer anpassbaren Eigenschaften in einer Datei mit den Topologieeigenschaften definiert. Eine Topologievorlagendatei stellt die Topologiestruktur bereit.

Der Befehl **parameterizeTopology** verwendet die in der Datei mit den Topologieeigenschaften definierten Name/Wert-Paare und die in der Topologievorlagendatei bereitgestellte Struktur und erstellt eine gültige Topologiedatei, die dann während der Installation verwendet wird.

IBM Intelligent Operations Center stellt die folgenden Topologiedateien bereit:

Dateiname	Zweck
Installationsausgangsverzeichnis/ioc/resource/custom.properties	Definiert die Position der Installationsmedien, Arbeitsverzeichnisse und anderer Eigenschaften. Diese Datei kann bearbeitet werden, um den Anforderungen der Umgebung des Kunden zu entsprechen.
Installationsausgangsverzeichnis/ioc/topology/iop_lite_topo.properties	Definiert die vom Kunden anpassbaren Eigenschaften für die Implementierung, einschließlich Hostnamen und Kennwörtern. Diese Datei kann bearbeitet werden, um den Anforderungen der Umgebung des Kunden zu entsprechen.
Installationsausgangsverzeichnis/ioc/topology/iop_lite_topo.template.xml	Definiert die Struktur der zu implementierenden Topologie. Die Datei verwendet die in der Eigenschaftendatei definierten Werte. Diese Datei sollte nicht bearbeitet werden.
Installationsausgangsverzeichnis/ioc/topology/iop_lite_topo.xml	Definiert die Topologie, die implementiert werden soll. Diese Datei wird mithilfe der Informationen in der Eigenschaften- und Vorlagendatei durch den Befehl **parameterizeTopology** erstellt. Diese Datei sollte nicht bearbeitet werden, außer wenn dies für die Wiederherstellung nach einem Installationsfehler notwendig ist.
Installationsausgangsverzeichnis/ioc/topology/iop_lite_topo.chk	Definiert die vom Vorabprüfungstool zu verwendenden Regeln, um festzustellen, ob die Server für die Installation von IBM Intelligent Operations Center ordnungsgemäß konfiguriert sind. Diese Datei sollte nicht bearbeitet werden.

Zugehörige Tasks:

„Plattformsteuerungstool installieren" auf Seite 53
Das Plattformsteuerungstool wird verwendet, um die Serverumgebung von IBM Intelligent Operations Center zu verwalten. Das Tool wird getrennt vom Produkt installiert.

Datei mit den Topologieeigenschaften

Die Datei mit den Topologieeigenschaften definiert die vom Kunden anpassbaren Eigenschaften für die Implementierung von IBM Intelligent Operations Center. Diese Datei muss bearbeitet werden, um den Anforderungen der Umgebung des Kunden zu entsprechen. Eigenschaften aus der bereitgestellten Datei mit den Topologieeigenschaften, die hier nicht dokumentiert sind, sollten nicht geändert werden.

Speichern Sie nach der Änderung der Datei mit den Topologieeigenschaften eine Kopie an einer sicheren Position. Die Datei enthält sicherheitsrelevante Informationen wie Benutzernamen und Kennwörter für das System in Klartext. Wenn ein Unbefugter Zugriff auf diese Datei hat, hat er dadurch uneingeschränkten Zugriff auf das System.

Die Datei mit den Topologieeigenschaften kann nach der Installation auf die folgenden Arten verwendet werden:

- Als Repository für Kennwortinformationen, falls ein Kennwort vergessen wird.
- Als Repository für Kennwörter, wenn diese im System geändert werden. Die geänderte Datei mit den Topologieeigenschaften kann verwendet werden, um die vom Plattformsteuerungstool verwendeten Kennwörter zu aktualisieren.
- Als Backup für Installationsinformationen, falls das System neu installiert werden muss. Die Datei mit den Topologieeigenschaften kann verwendet werden, ohne dass alle Installationsparameter neu definiert werden müssen.

Zugehörige Tasks:

„Topologiedatei erstellen" auf Seite 45
Generieren Sie, bevor Sie die Installationsschritte für IBM Intelligent Operations Center ausführen, eine Topologiedatei mit den für die Installation erforderlichen Parametern.

Informationen zu Zielservern:

Im Abschnitt `SERVERS` der Datei mit den Topologieeigenschaften werden Eigenschaften für die Zielserver definiert.

Tabelle 16 zeigt die Eigenschaftswerte der Server an, die in der Datei mit den Topologieeigenschaften festgelegt werden können.

Tabelle 16. Eigenschaften der Zielserver

Eigenschaft	Beschreibung
`DB.1.HOST`	Der Hostname des Datenserver
`DB.1.ACCOUNT.PWD`	Das `root`-Kennwort für den Datenserver
`DB.1.SSH_PORT`	Die Portnummer für SSH-Zugriff zum Datenserver
`APP.1.HOST`	Der Hostname des Anwendungsserver
`APP.1.ACCOUNT.PWD`	Das `root`-Kennwort für den Anwendungsserver
`APP.1.SSH_PORT`	Die Portnummer für SSH-Zugriff zum Anwendungsserver
`EVENT.1.HOST`	Der Hostname des Ereignisserver
`EVENT.1.ACCOUNT.PWD`	Das `root`-Kennwort für den Ereignisserver
`EVENT.1.SSH_PORT`	Die Portnummer für SSH-Zugriff zum Ereignisserver
`MGMT.1.HOST`	Der Hostname des Verwaltungsserver

Tabelle 16. Eigenschaften der Zielserver (Forts.)

Eigenschaft	Beschreibung
MGMT.1.ACCOUNT.PWD	Das root-Kennwort für den Verwaltungsserver
MGMT.1.SSH_PORT	Die Portnummer für SSH-Zugriff zum Verwaltungsserver

Wichtig: Hostnamenwerte müssen vollständig qualifizierte Hostnamen sein, die der festgelegten Groß-/Kleinschreibung entsprechend eingegeben werden. Beispiel: IOC15App.IOC15.com ist nicht das Gleiche wie ioc15app.ioc15.com.

Eine SSH-Portnummer kann für jeden Server eingestellt werden. Aber die konfigurierten Portnummern werden nur vom Plattformsteuerungstool verwendet. Port 22 muss für SSH-Zugriff auf jedem Server aktiviert sein. Port 22 ist für SSH-Zugriff durch IBM Intelligent Operations Center während der Installation erforderlich.

Informationen zu Verzeichnisservices:

Die Datei mit den Topologieeigenschaften definiert Werte, die für die Verschlüsselung von Benutzerkennwörtern und anderen sensiblen Daten innerhalb des Verzeichnisses verwendet werden.

Die Verschlüsselung basiert auf zwei Werten: LDAP.SEED und LDAP.SALT.

Bei den Werten muss es sich um druckbare ASCII-Zeichen handeln. Druckbare ASCII-Zeichen sind Zeichen mit Codepunktwerten zwischen 33 und 126. Leerzeichen können nicht verwendet werden.

Tabelle 17. Eigenschaften von Verzeichnisservices

Eigenschaft	Beschreibung
LDAP.SEED	Eine aus 12 bis 1016 druckbaren ASCII-Zeichen bestehende Zeichenfolge zwischen den Codepunkten 33 und 126. Es sollte eine kryptografisch starke Zeichenfolge verwendet werden. Beispielsweise eine lange Zeichenfolge mit Buchstaben in Groß-/Kleinschreibung, Zahlen und Sonderzeichen ohne allgemeine Wörter oder Wortfolgen.
LDAP.SALT	Eine aus 12 druckbaren ASCII-Zeichen bestehende Zeichenfolge zwischen den Codepunkten 33 und 126. **Wichtig:** LDAP.SALT muss exakt 12 Zeichen lang sein. Ein mehr oder weniger Zeichen umfassender Wert führt dazu, dass die Installation fehlschlägt.

Dokumentieren Sie die Werte LDAP.SEED und LDAP.SALT außerhalb des Systems. Die Werte sind erforderlich, wenn Sie die Verzeichniseinträge exportieren oder replizieren müssen.

Kennwortinformationen:

Kennwörter für mehrere Benutzer-IDs, die in der IBM Intelligent Operations Center-Lösung verwendet werden, sind in der Datei mit den Topologieeigenschaften definiert. Aus Sicherheitsgründen sollten die mit IBM Intelligent Operations Center ausgelieferten Standardkennwörter geändert werden.

Kennwörter können nur alphanumerische Zeichen (a-z, A-Z, 0-9) enthalten. Sofern nicht anders vorgegeben, dürfen Kennwörter eine Länge von höchstens 30 Zeichen haben.

Tabelle 18. Kennworteigenschaften

Eigenschaft	Zugehöriger Benutzername	Beschreibung
LDAP.DB.PWD	dsrdbm01	Datenbank des LDAP-Verzeichnisses
LDAP.ADMIN.DN.PWD	cn=root	Bindung des LDAP-Administrators
LDAP.BIND.DN.PWD	cn=bind	LDAP-Bindung
LDAP.PROXY.INSTANCE.PWD	tdsproxy	LDAP-Proxyinstanz
LDAP.PROXY.ADMIN.DN.PWD	cn=root	Bindung des LDAP-Proxyadministrators
LDAP.PROXY.BIND.DN.PWD	cn=bind	LDAP-Proxybindung
TAM.SECMASTER.PWD	none	Masterkennwort des Sicherheitsservice Dieser Benutzer verfügt auf den Zielservern über dieselben Berechtigungen wie der root-Benutzer. Stellen Sie aufgrund des Zugriffs, der diesem Benutzer zur Verfügung gestellt wird, sicher, dass das Kennwort ein langer Wert ist, sich von anderen Kennwörtern unterscheidet und sicher aufbewahrt wird.
TAM.WEBSEAL.ADMIN.PWD	sec_master	Administrator des Sicherheitsservice Dieser Benutzer verfügt auf den Zielservern über dieselben Berechtigungen wie der root-Benutzer. Stellen Sie aufgrund des Zugriffs, der diesem Benutzer zur Verfügung gestellt wird, sicher, dass das Kennwort ein langer Wert ist, sich von anderen Kennwörtern unterscheidet und sicher aufbewahrt wird.
WBM.DB.USER.PWD	db2ibm	Servicedatenbank für die Überwachung von Geschäftsaktivitäten
WODM.DB.USER.PWD	db2wodm	Servicedatenbank für das Entscheidungsmanagement
WODM.ADMIN.UID.PWD	resAdmin1	Serviceadministrator für das Decision Management
WODM.DEPLOYER.UID.PWD	resDeployer1	Implementierungsprogramm für die Serviceregeln des Decision Management
WODM.MONITOR.UID.PWD	resMonitor1	Servicemonitor für das Decision Management
WODM.DB.DC.USER.PWD	wodmdc	Datenbankkonsole für das Decision Management
WODM.rtsAdmin.UID.PWD	rtsAdmin	Konsolenadministrator für das Decision Management
WODM.rtsConfig.UID.PWD	rtsConfig	Konsolenkonfiguration für das Decision Management
WODM.rtsUser.UID.PWD	rtsUser	Konsolenbenutzer für das Decision Management
UDDI.DB.USER.PWD	db2uddi	UDDI-Servicedatenbank

Tabelle 18. Kennworteigenschaften (Forts.)

Eigenschaft	Zugehöriger Benutzername	Beschreibung
IHS.KEYSTORE.PWD	none	Schlüsselspeicher des HTTP-Servers
WAS.ADMIN.ACCOUNT.PWD	waswebadmin	Administrator der Anwendungsservices
WAS.LTPA.PWD	keine	LTPA-Token
PORTAL.ADMIN.ACCOUNT.PWD	waswebadmin	Administrator für die WebSphere Application Server-Konsole für den WebSphere Portal-Server
PORTAL.ADMIN.UID.PWD	wpsadmin	Administrator für den WebSphere Portal-Server
PORTAL.DB.USER.PWD	db2port1	WebSphere Portal-Datenbank
OMNIBUS.ADMIN.ACCOUNT.PWD	netcool	Administrator für Ereignisservices
IMPACT.WAS.ACCOUNT.PWD	wasadmin	Administrator für Systemereignisservices
TSRM.WAS.ADMIN.PWD	waswebadmin	Administrator für den Serviceanforderungsmanager
TSRM.DB.USER.PWD	maximo	Datenbank des Serviceanforderungsmanagers
TSRM.ADMIN.USER.PWD	maxadmin	Administrator für den Serviceanforderungsmanager
TSRM.REG.USER.PWD	maxreg	Benutzer des Serviceanforderungsmanagers
TSRM.INITADM.USER.PWD	maxintadm	Integrationsbenutzer des Serviceanforderungsmanagers
MGMT.WAS.ADMIN.PWD	waswebadmin	Administrator der Anwendungsservices
TEPS.DB.USER.PWD	itmuser	Datenbank des Unternehmensportals
TIM.STORE.PWD	keine	Speicher des Identitätsmanagements
TIM.ADMIN.USER.PWD	waswebadmin	Administrator des Identitätsmanagers
DOMINO.USER.PWD	notes	Benutzer der Zusammenarbeit
DOMINO.ORG.PWD	IBM	Organisation der Zusammenarbeit
DOMINO.ADMIN.PWD	notes admin	Administrator der Zusammenarbeit
DOMINO.ST.ADMIN.PWD	wpsadmin	Portaladministrator der Zusammenarbeit
DOMINO.ST.BIND.PWD	wpsbind	LDAP-Bindung der Zusammenarbeit
DEFAULT.PWD.DAS	dausr1, dausr2, dausr3, dausr4, dausr5, dausr6, dausr7, dausr8	Administrationsserver der Datenbankservices
DEFAULT.PWD.DB2	db2inst1, db2inst2, db2inst3, db2inst4, db2inst5, db2inst6, db2inst7, db2inst8	Datenserver der Datenbankservices
DEFAULT.PWD.IHS	ihsadmin	HTTP-Server
DEFAULT.PWD.MQM	mqm	Benutzer der Nachrichtenübertragungsservices
MQM.CONN.USER.PWD	mqmconn	Verbindung der Nachrichtenübertragungsservices
DEFAULT.PWD.TAI	taiuser	Sicherheit der Anwendungsservices

Tabelle 18. Kennworteigenschaften (Forts.)

Eigenschaft	Zugehöriger Benutzername	Beschreibung
`ITM.ADMIN.PWD`	sysadmin	Administrator des Systemmanagements **Einschränkung:** Das Kennwort darf höchstens 15 Zeichen umfassen.
`IOP.ADMIN.USER.PWD`	ibmadmin	Systemverwaltungstools Dieser Benutzer verfügt auf den Zielservern über dieselben Berechtigungen wie der `root`-Benutzer. Das Plattformsteuerungstool wird unter diesem Benutzernamen ausgeführt. Stellen Sie aufgrund des Zugriffs, der diesem Benutzer zur Verfügung gestellt wird, sicher, dass das Kennwort ein langer Wert ist, sich von anderen Kennwörtern unterscheidet und sicher aufbewahrt wird.
`IOP.USER.USER.PWD`	ibmuser	Endbenutzer des Systems

Zugehörige Konzepte:

Kapitel 3, „Schutz der Lösung", auf Seite 73
Da das IBM Intelligent Operations Center bei entscheidenden Vorgängen eine zentrale Rolle einnimmt, ist die Sicherheit ein wichtiger Faktor. Zur Gewährleistung der Sicherheit ist es wichtig, dass Sie die Standardeinstellungen kennen. Auch die Verwaltung der Benutzer der Lösung ist unerlässlich, um allen Benutzern die jeweils richtige Zugriffsebene zuzuweisen.

Zugehörige Tasks:

„Installationseigenschaften anpassen" auf Seite 37
Die Datei mit den Installationseigenschaften und die Dateien mit den Topologieeigenschaften stellen Definitionen bereit, die von den Installationsscripts benötigt werden.

Zugehörige Verweise:

„Musterbenutzer" auf Seite 75
Während der Implementierung des IBM Intelligent Operations Center werden Musterbenutzer erstellt.

Topologiekennwort erstellen

Das Topologiekennwort wird während des Installationsprozesses verwendet, um die Datei, die die Lösungstopologie definiert, zu verschlüsseln und um auf sie zuzugreifen.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

1. Melden Sie sich als `root` an oder wechseln Sie zum Root-Account, indem Sie den Befehl **`su -`** ausführen.
2. Führen Sie den Befehl **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`** aus.
3. Wechseln Sie in das Verzeichnis *`Installationsausgangsverzeichnis`*`/ioc`.

4. Führen Sie den Befehl **bin/ba.sh createSecretKey -p** *Kennwort* aus, wobei *Kennwort* das Kennwort ist, das für die Topologie erstellt werden soll. Mit diesem Befehl wird die Datei *Installationsausgangsverzeichnis*/ioc/resource/ioc.keystore erstellt. Diese Datei enthält den Schlüssel, der zur Verschlüsselung der Datei mit den Topologieeigenschaften verwendet wird. Die Datei ioc.keystore wird auch mit dem im Befehl **createSecretKey** festgelegten Kennwort verschlüsselt. Um das Kennwort und den Schlüssel für die Installation zu ändern, löschen Sie die Datei *Installationsausgangsverzeichnis*/ioc/resource/ioc.keystore, und führen Sie dann den Befehl **createSecretKey** erneut aus. Notieren Sie sich das Kennwort zur Verwendung in anderen Installationsschritten.

Zugehörige Tasks:

„Topologiedatei erstellen"
Generieren Sie, bevor Sie die Installationsschritte für IBM Intelligent Operations Center ausführen, eine Topologiedatei mit den für die Installation erforderlichen Parametern.

Topologiedatei erstellen

Generieren Sie, bevor Sie die Installationsschritte für IBM Intelligent Operations Center ausführen, eine Topologiedatei mit den für die Installation erforderlichen Parametern.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

1. Melden Sie sich als root an oder wechseln Sie zum Root-Account, indem Sie den Befehl **su -** ausführen.
2. Führen Sie den Befehl **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** aus.
3. Gehen Sie zum Verzeichnis *Installationsausgangsverzeichnis*/ioc/topology.
4. Bearbeiten Sie die Datei iop_lite_topo.properties, und nehmen Sie alle Änderungen vor, die für Ihre Umgebung erforderlich sind.
5. Kopieren Sie die Topologievorlagendatei in die Topologiedatei, indem Sie den Befehl **cp iop_lite_topo.template.xml iop_lite_topo.xml** ausführen.
6. Wechseln Sie in das Verzeichnis *Installationsausgangsverzeichnis*/ioc.
7. Führen Sie den Befehl **bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/ iop_lite_topo.properties -p** *Kennwort* aus, wobei *Kennwort* das Topologiekennwort ist. Die in der Datei mit den Topologieeigenschaften definierten Parameter werden auf die Topologiedatei angewendet.
8. Optional: Um Kennwörter in der Topologiedatei zu verschlüsseln, führen Sie den Befehl **bin/ba.sh encryptTopology -t iop_lite_topo -p** *Kennwort* aus. Dabei ist *Kennwort* das Topologiekennwort.

   Wichtig: Es werden nur die Kennwörter in der Topologiedatei verschlüsselt. Kennwörter in anderen Dateien, z. B. der Datei mit den Topologieeigenschaften, werden nicht verschlüsselt.

Zugehörige Konzepte:

„Datei mit den Topologieeigenschaften" auf Seite 40
Die Datei mit den Topologieeigenschaften definiert die vom Kunden anpassbaren Eigenschaften für die Implementierung von IBM Intelligent Operations Center. Diese Datei muss bearbeitet werden, um den Anforderungen der Umgebung des Kunden zu entsprechen. Eigenschaften aus der bereitgestellten Datei mit den Topologieeigenschaften, die hier nicht dokumentiert sind, sollten nicht geändert werden.

Zugehörige Tasks:

„Topologiekennwort erstellen" auf Seite 44
Das Topologiekennwort wird während des Installationsprozesses verwendet, um die Datei, die die Lösungstopologie definiert, zu verschlüsseln und um auf sie zuzugreifen.

Vorabprüfungstool ausführen

Überprüfen Sie durch Ausführung des Vorabprüfungstools vor dem Hochladen von Installationspaketen auf die Zielserver, dass die Zielserver bereit für die Installation sind.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

1. Melden Sie sich als `root` an oder wechseln Sie zum Root-Account, indem Sie den Befehl **`su -`** ausführen.
2. Führen Sie den Befehl **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`** aus.
3. Wechseln Sie in das Verzeichnis *`Installationsausgangsverzeichnis`*`/ioc`.
4. Führen Sie den Befehl **`bin/ba.sh precheckTopology -t iop_lite_topo -p`** *Kennwort* aus, wobei *Kennwort* das Topologiekennwort ist. Für jede Vorabprüfung auf jedem Server werden Nachrichten angezeigt. Der Status jeder Prüfung ist entweder `[Pass]` (bestanden) oder `[Fail]` (fehlgeschlagen). Nach Ausführung aller Tests wird eine Zusammenfassung aller fehlgeschlagenen Tests angezeigt.
5. Wenn Fehler vorhanden sind, führen Sie die entsprechende Maßnahme durch, um das Problem zu beheben, und führen Sie das Vorabprüfungstool erneut aus, bis keine Fehler mehr vorhanden sind.

Ergebnisse

Wenn die Nachricht CHK0101W ausgegeben wird, ist kein DNS-Server vorhanden, der für die Umgebung konfiguriert ist, oder der DNS-Server hat Ihre Server nicht definiert. Diese Warnung kann ignoriert werden, wenn Ihre Server unter Verwendung der statischen IP-Adressierung in der Datei `/etc/hosts` definiert werden.

Zugehörige Konzepte:

„TCP/IP-Netz einrichten" auf Seite 23
Vor der Installation von IBM Intelligent Operations Center muss das TCP/IP-Netz zwischen den Servern ordnungsgemäß eingerichtet werden.

Linux-Sicherheitseinstellungen

Linux-Sicherheitseinstellungen müssen geändert werden, um das Plattformsteuerungstool zu aktivieren.

Diese Einstellungen können durch das Ausführen einer Reihe von Befehlen oder durch die Verwendung eines Scripts geändert werden.

Das Script nimmt die von den Befehlen angegebenen Änderungen vor. Wenn die Befehle nicht die Anforderungen Ihrer Installation erfüllen oder wenn die Unternehmensprozesse keine Sicherheitsänderungen durch das Script zulassen, ändern Sie die Einstellungen mithilfe individueller Befehle.

Linux-Sicherheitseinstellungen manuell anpassen

Die erforderlichen Linux-Sicherheitseinstellungen können durch Ausführen einer Reihe von Befehlen vorgenommen werden.

Vorgehensweise

1. Melden Sie sich auf dem Installationsserver als `root` an oder wechseln Sie mit dem Befehl **`su -`** zum Root-Account.
2. Gehen Sie wie folgt vor, um das Plattformsteuerungstool zu aktivieren. Diese Schritte müssen für jeden der folgenden Zielserver ausgeführt werden:
   - Anwendungsserver
   - Datenserver
   - Ereignisserver
   - Verwaltungsserver

   a. Führen Sie den Befehl **`visudo`** aus. Die Datei `/etc/sudoers` wird geöffnet und kann bearbeitet werden.

   b. Geben Sie den Buchstaben `i` ein, um in den Einfügemodus zu wechseln, in dem Änderungen an der Datei vorgenommen werden können.

   c. Suchen Sie nach der folgenden Zeile:

   ```
   #%wheel ALL=(ALL) NOPASSWD: ALL
   ```

   Ändern Sie diese Zeile in:

   ```
   %wheel ALL=(ALL) NOPASSWD: ALL
   ```

   d. Fügen Sie am Ende der Datei die folgende Zeile hinzu:

   ```
   Defaults:%wheel !requiretty
   ```

   e. Drücken Sie die Abbruchtaste (Esc). Der Einfügemodus wird beendet.

   f. Geben Sie `:wq` ein. Die Datei wird gespeichert.

   g. Führen Sie den Befehl **`exit`** aus. Die Anmeldeanzeige des Installationsservers wird wieder anzeigt.

   Nach Ausführung dieser Schritte für alle vier Server lassen die Linux-Sicherheitsfunktionen es zu, dass Benutzer der Gruppe `wheel` mit dem Befehl **`sudo`** Systembefehle lokal oder über eine ferne Sitzung ausführen.

Zugehörige Tasks:

„Linux-Sicherheitseinstellungen mit einem Script anpassen"
Die erforderlichen Linux-Sicherheitseinstellungen können durch das Ausführen eines Scripts vorgenommen werden.

Linux-Sicherheitseinstellungen mit einem Script anpassen

Die erforderlichen Linux-Sicherheitseinstellungen können durch das Ausführen eines Scripts vorgenommen werden.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *`Installationsausgangsverzeichnis`*`/ioc`.

2. Führen Sie den Befehl **bin/install-prepare-env.sh -d***Installationsausgangsverzeichnis***/ioc -f topology/iop_lite_topo.properties -p***Kennwort* aus. Dabei ist *Kennwort* das Topologiekennwort.

Zugehörige Tasks:

„Linux-Sicherheitseinstellungen manuell anpassen" auf Seite 47
Die erforderlichen Linux-Sicherheitseinstellungen können durch Ausführen einer Reihe von Befehlen vorgenommen werden.

Der Befehl "installTopology" (Topologie installieren)

Der Befehl **installTopology** verwendet die Informationen in der Topologiedatei, um IBM Intelligent Operations Center zu installieren.

Bevor er die Topologiedatei für die Installation von IBM Intelligent Operations Center verwendet, überprüft der Befehl **installTopology**, dass die Installationsdateien auf die Zielserver kopiert wurden. Falls die Dateien nicht kopiert wurden, kopiert der Befehl **installTopology** die erforderlichen Dateien, bevor der Vorgang fortgesetzt wird.

Mithilfe der Topologiedatei als Leitfaden installiert der Befehl **installTopology** jede Komponente von IBM Intelligent Operations Center und führt alle erforderlichen Konfigurationen durch. Während der Installation werden Nachrichten zum Installationsfortschritt angezeigt.

Sollte während der Verarbeitung des Befehls **installTopology** ein Fehler auftreten, kann die Installation möglicherweise erneut gestartet werden, nachdem die Ursache für das Fehlschlagen einer oder mehrerer Komponenteninstallationen festgestellt wurde. Fehlgeschlagene Installationen werden durch den Installationsstatus in der Topologiedatei angezeigt.

Anmerkung: Für eine virtuelle Umgebung ist es empfehlenswert, vor dem Ausführen des Befehls **installTopology** und nach jeder erfolgreichen Installation eine Momentaufnahme zu erstellen.

Installationsstatus

Das Attribut **Status** der Topologiedatei zeigt den Installationsstatus jeder Komponente an. Wenn der Befehl **installTopology** ausgeführt wird, wird je nach Status der Komponente die in Tabelle 19 angegebene Aktion ausgeführt.

Tabelle 19. Installationsstatus und Aktionen

Wert	Status	Aktion "installTopology" (Topologie installieren)
New	Die Komponente wurde nicht installiert.	Der Status wird auf Uncertain (Unsicher) geändert und die Komponente wird installiert. Wenn die Komponenteninstallation erfolgreich war, wird der Status auf Ready (Bereit) geändert.
Ready	Die Komponente wurde erfolgreich installiert.	Die Installation der Komponente wird übersprungen, wenn der Befehl **installTopology** erneut ausgeführt wird.
Uncertain	Die Komponente ist nicht erfolgreich installiert worden oder die Installation ist noch nicht abgeschlossen.	Die Komponente wird installiert. Wenn die Komponenteninstallation erfolgreich war, wird der Status auf Ready geändert.

Optionen für die Installation von Komponenten des IBM Intelligent Operations Center

Die Installation von IBM Intelligent Operations Center kann mehrere Stunden dauern. Aufgrund der Länge der benötigten Zeit kann IBM Intelligent Operations Center in einer oder in mehreren Phasen installiert werden.

Bei einer Installation, die in einer einzigen Phase durchgeführt wird, wird der Installationsprozess ausgeführt, bis alle Komponenten installiert sind oder bis es zu einem Fehler bei der Installation kommt. Wenn die Installation fehlschlägt, muss sie von Anfang an neu gestartet werden.

Bei einer Installation mit mehreren Phasen ist der Installationsprozess in drei unterschiedliche Phasen aufgeteilt:

uploadTopology (Topologie hochladen)
Kopiert die Installationsdateien vom Installationsserver auf die Zielserver.

Phase 1
Installiert manche der Komponenten von IBM Intelligent Operations Center und erstellt damit eine Basis für die Installation der verbleibenden Komponenten.

Phase 2
Installiert die verbleibenden Komponenten von IBM Intelligent Operations Center.

Wenn die Ausführung in einer virtuellen Umgebung stattfindet, sollte für den Fall, dass ein Neustart erforderlich ist, nach jeder Phase eine Momentaufnahme erstellt werden.

Die Phase **uploadTopology** wird als separater Befehl ausgeführt. Wenn die Installationsdateien bereits auf die Zielserver kopiert wurden, werden sie nicht nochmal kopiert.

Die auszuführenden Phasen sind in der Datei mit den Topologieeigenschaften definiert. Die Eigenschaften **Status.Phase1** und **Status.Phase2** bestimmen, ob die Installationsphasen ausgeführt werden, wenn der Befehl **installTopology** ausgeführt wird. Wenn sie auf New (Neu) gesetzt sind, wird die Phase ausgeführt. Wenn sie auf Ready (Bereit) gesetzt sind, wird die Phase übersprungen.

Die IBM Intelligent Operations Center-Architektur in einer einzelnen Phase installieren

Die mit IBM Intelligent Operations Center verwendete Architektur kann in einer einzigen Phase installiert werden. Wenn Sie in einer virtuellen Umgebung installieren, ist es bei Ausführung der Installation in einer einzelnen Phase nicht möglich, während des Installationsprozesses Momentaufnahmen zu erstellen.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

1. Öffnen Sie auf dem Installationsserver ein Terminalfenster und melden Sie sich als `root` an. Sind Sie nicht als `root` angemeldet, wechseln Sie mit dem Befehl **su -** zum `root`-Account.
2. Kopieren Sie die für die Installation erforderlichen Dateien auf die Zielserver und installieren Sie IBM Intelligent Operations Center.
   a. Wechseln Sie in das Verzeichnis *Installationsausgangsverzeichnis*`/ioc`.
   b. Führen Sie den Befehl **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** aus.
   c. Führen Sie den Befehl **bin/ba.sh installTopology -t iop_lite_topo -p** *Kennwort* aus, wobei *Kennwort* das Topologiekennwort ist.

   Die erforderlichen Installationsdateien werden auf die Zielserver kopiert und IBM Intelligent Operations Center wird installiert.

   Es werden Nachrichten angezeigt, die Aufschluss über den Installationsfortschritt geben. In diesen Nachrichten wird der Status der installierten Komponente angegeben. Folgende Statusangaben sind möglich:

   [OK] Die Komponente wurde erfolgreich installiert.

[Fail] (fehlgeschlagen)
Die Installation der Komponente ist fehlgeschlagen.

Ergebnisse

Der Installationsprozess kann bis zu 14 Stunden dauern. Die IBM Intelligent Operations Center-Architektur wurde erfolgreich installiert, wenn alle Nachrichten mit dem Status `[ OK ]` enden.

IBM Intelligent Operations Center-Architektur in mehreren Phasen installieren

Die mit IBM Intelligent Operations Center verwendete Architektur kann in mehreren Phasen installiert werden. Eine Installation mit mehreren Phasen ermöglicht es Ihnen, Installationsprobleme schneller zu lösen, anstatt auf die Beendigung des gesamten Installationsprozesses zu warten. Wenn Sie die Installation in einer virtualisierten Umgebung durchführen, ist es Ihnen durch die Installation in mehreren Phasen außerdem möglich, während des Installationsprozesses Momentaufnahmen zu erstellen.

Informationen zu diesem Vorgang

Wichtig: Schalten Sie die Server zwischen den Installationsphasen nicht herunter. Das Herunterfahren von Servern zwischen Installationsphasen wurde nicht getestet und kann zu unvorhersehbaren Ergebnissen führen.

Vorgehensweise

1. Öffnen Sie auf dem Installationsserver ein Terminalfenster und melden Sie sich als `root` an. Sind Sie nicht als `root` angemeldet, wechseln Sie mit dem Befehl **`su -`** zum `root`-Account.
2. Führen Sie den Befehl **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`** aus.
3. Kopieren Sie die Installationsdateien auf die Zielserver.
   a. Wechseln Sie in das Verzeichnis *`Installationsausgangsverzeichnis`*`/ioc`.
   b. Führen Sie den Befehl **`bin/ba.sh uploadImage -t iop_lite_topo -threadCount 4 -p`** *Kennwort* aus. Dabei ist *Kennwort* das Topologiekennwort. Der Parameter **`-threadCount`** legt die Zahl der Threads fest, die verwendet werden, wenn die Installationsdateien kopiert werden. Der Wert kann bei Bedarf geändert werden.

   Die für jeden Zielserver erforderlichen Dateien werden vom Installationsserver auf die Zielserver kopiert. Dieser Schritt kann bis zu 2 Stunden dauern.

   Es werden Nachrichten angezeigt, die den Uploadfortschritt angeben. Die Nachrichten geben den Status der hochgeladenen Komponente an. Folgende Statusangaben sind möglich:

   [OK] Komponente erfolgreich hochgeladen.

   [Fail] (fehlgeschlagen)
   Upload der Komponente fehlgeschlagen.
4. Optional: Wenn Sie die Installation in einer virtualisierten Umgebung durchführen, erstellen Sie eine Momentaufnahme von allen Zielservern. Fahren Sie die virtuellen Maschinen herunter, bevor Sie die Momentaufnahme erstellen, um Festplattenspeicher und Verarbeitungszeit zu sparen. Starten Sie die virtuellen Maschinen neu, nachdem Sie die Momentaufnahme erstellt haben. Die Momentaufnahme kann verwendet werden, um die Installation von dieser Stelle aus neu zu starten, falls im Laufe von aufeinanderfolgenden Installationsprozessen Fehler auftreten.
5. Bereiten Sie die Ausführung von Installationsphase 1 vor.
   a. Bearbeiten Sie mithilfe eines Texteditors die Datei mit den Topologieeigenschaften: *`Installationsausgangsverzeichnis`*`/ioc/topology/iop_lite_topo.properties`.
   b. Ändern Sie die Statuswerte wie angezeigt:

   ```
   Status.Phase1="New"
   Status.Phase2="Ready"
   ```

Dadurch wird dem Installationsprogramm mitgeteilt, dass es die erste Phase installieren und die zweite Phase überspringen soll.

c. Wechseln Sie in das Verzeichnis *Installationsausgangsverzeichnis*/ioc.

d. Führen Sie den Befehl **cp topology/iop_lite_topo.template.xml topology/iop_lite_topo.xml** aus. Die Topologievorlagendatei wird in die Topologiedatei kopiert.

e. Führen Sie den Befehl **bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p***Kennwort* aus. Dabei ist *Kennwort* das Topologiekennwort. Die in der Datei mit den Topologieeigenschaften definierten Eigenschaftswerte werden auf die Topologiedatei angewendet.

f. Optional: Führen Sie den Befehl **bin/ba.sh encryptTopology -t iop_lite_topo -p***Kennwort* aus. Dabei ist *Kennwort* Ihr Topologiekennwort. Die Kennwörter in der Topologiedatei werden mithilfe des bereitgestellten Topologiekennwortes verschlüsselt.

6. Führen Sie Installationsphase 1 aus.

a. Wechseln Sie in das Verzeichnis *Installationsausgangsverzeichnis*/ioc.

b. Führen Sie den Befehl **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** aus.

c. Führen Sie den Befehl **bin/ba.sh installTopology -t iop_lite_topo -p** *Kennwort* aus, wobei *Kennwort* das Topologiekennwort ist.

Das Installationsprogramm installiert Basiskomponenten, die für IBM Intelligent Operations Center erforderlich sind. Dieser Schritt kann bis zu 9 Stunden dauern.

Es werden Nachrichten angezeigt, die Aufschluss über den Installationsfortschritt geben. In diesen Nachrichten wird der Status der installierten Komponente angegeben. Folgende Statusangaben sind möglich:

[OK] Die Komponente wurde erfolgreich installiert.

[Fail] (fehlgeschlagen)
Die Installation der Komponente ist fehlgeschlagen.

7. Optional: Wenn Sie die Installation in einer virtualisierten Umgebung durchführen, erstellen Sie eine Momentaufnahme von allen Zielservern. Schalten Sie die virtuellen Server nicht ab, bevor Sie nicht die Momentaufnahmen erstellt haben. Schließen Sie, wenn Sie die Momentaufnahme erstellen, eine Momentaufnahme von einem Hauptspeicher einer virtuellen Maschine mit ein. Die Momentaufnahme kann verwendet werden, um die Installation von dieser Stelle aus neu zu starten, falls im Laufe von nachfolgenden Installationsprozessen Fehler auftreten.

8. Bereiten Sie die Ausführung von Installationsphase 2 vor.

a. Bearbeiten Sie mithilfe eines Texteditors die Datei mit den Topologieeigenschaften: *Installationsausgangsverzeichnis*/ioc/topology/iop_lite_topo.properties.

b. Ändern Sie die Statuswerte wie angezeigt:

```
Status.Phase1="Ready"
Status.Phase2="New"
```

Dadurch wird dem Installationsprogramm mitgeteilt, dass es die zweite Phase installieren und die erste Phase überspringen soll.

c. Wechseln Sie in das Verzeichnis *Installationsausgangsverzeichnis*/ioc.

d. Führen Sie den Befehl **cp topology/iop_lite_topo.template.xml topology/iop_lite_topo.xml** aus. Die Topologievorlagendatei wird in die Topologiedatei kopiert.

e. Führen Sie den Befehl **bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p***Kennwort* aus. Dabei ist *Kennwort* das Topologiekennwort. Die in der Datei mit den Topologieeigenschaften definierten Eigenschaftswerte werden auf die Topologiedatei angewendet.

f. Optional: Führen Sie den Befehl **bin/ba.sh encryptTopology -t iop_lite_topo -p***Kennwort* aus. Dabei ist *Kennwort* Ihr Topologiekennwort. Die Kennwörter in der Topologiedatei werden mithilfe des bereitgestellten Topologiekennwortes verschlüsselt.

9. Führen Sie Installationsphase 2 aus.
   a. Wechseln Sie in das Verzeichnis *Installationsausgangsverzeichnis*/ioc.
   b. Führen Sie den Befehl **export JAVA_HOME=/opt/ibm/java-x86_64-60/jre** aus.
   c. Führen Sie den Befehl **bin/ba.sh installTopology -t iop_lite_topo -p** *Kennwort* aus, wobei *Kennwort* das Topologiekennwort ist.

   Das Installationsprogramm installiert die verbleibenden Komponenten, die für IBM Intelligent Operations Center erforderlich sind. Dieser Schritt kann bis zu 4 Stunden dauern.

   Es werden Nachrichten angezeigt, die Aufschluss über den Installationsfortschritt geben. In diesen Nachrichten wird der Status der installierten Komponente angegeben. Folgende Statusangaben sind möglich:

   [OK] Die Komponente wurde erfolgreich installiert.

   [Fail] (fehlgeschlagen)
   Die Installation der Komponente ist fehlgeschlagen.

Ergebnisse

Die IBM Intelligent Operations Center-Architektur wurde erfolgreich installiert, wenn alle Nachrichten mit dem Status `[ OK ]` enden.

Installation der IBM Intelligent Operations Center-Architektur während einer schrittweisen Installation neu starten

Wenn die Architekturinstallation fehlschlägt, kann die Installation neu gestartet werden.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um eine fehlgeschlagene Installation neu zu starten.

Vorgehensweise

1. Bearbeiten Sie die Topologiedatei, um zu bestimmen, welche Komponente fehlgeschlagen ist. Dies wird durch `Status="Uncertain"` angezeigt.
2. Bestimmen und beheben Sie die Fehlerursache. Mithilfe des MustGather-Installationstools können Sie die Installationsprotokolle für die Überprüfung sammeln.
3. Führen Sie den Befehl **installTopology** erneut aus. Es wird erneut versucht, die Installation durchzuführen. Alle Komponenten mit `Status="New"` und `Status="Uncertain"` werden installiert. Komponenten mit `Status="Ready"` wurden bereits erfolgreich installiert und werden übersprungen.

Nächste Schritte

Manchmal wird eine einmal fehlgeschlagen Komponenteninstallation nicht erfolgreich installiert. In diesem Fall müssen Sie zunächst die Umgebung erneut erstellen, die vorhanden war, bevor der Befehl **installTopology** ausgeführt wurde, und die Installation dann erneut starten. Für eine Umgebung mit Virtualisierung können Momentaufnahmen der Umgebung verwendet werden, um das System schnell in den Zustand zurückzusetzen, in dem es sich befand, bevor der Befehl **installTopology** ausgeführt wurde.

Zugehörige Tasks:

„MustGather-Tool bei der Installation ausführen" auf Seite 316
Es werden Protokolldateien erstellt, während IBM Intelligent Operations Center installiert wird. Es ist ein Tool verfügbar, das diese Protokolldateien zur Analyse zusammenstellt.

Plattformsteuerungstool installieren

Das Plattformsteuerungstool wird verwendet, um die Serverumgebung von IBM Intelligent Operations Center zu verwalten. Das Tool wird getrennt vom Produkt installiert.

Vorbereitende Schritte

Das Produkt IBM Intelligent Operations Center muss bereits vor Installation des Plattformsteuerungstool installiert sein.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

1. Öffnen Sie auf dem Installationsserver ein Terminalfenster und melden Sie sich als `root` an. Sind Sie nicht als `root` angemeldet, wechseln Sie mit dem Befehl **`su -`** zum `root`-Account.
2. Wechseln Sie in das Verzeichnis *`install_home`*`/isp/mgmt/setup`.
3. Führen Sie den Befehl **`./iopmgmt-install.sh -f`** *Installationsausgangsverzeichnis*`/ioc/topology/iop_lite_topo.properties -p` *Kennwort* aus. Dabei ist *Kennwort* das von Ihnen gewählte Kennwort für den Zugriff auf das Tool. Merken Sie sich dieses Kennwort, da Sie es für die Ausführung des Tools benötigen. Das Plattformsteuerungstool ist erfolgreich auf dem Verwaltungsserver installiert, wenn für alle installierten Komponenten der Status `[ OK ]` angezeigt wird.
4. Optional: Wenn Sie das vom IBM Intelligent Operations Center bereitgestellte Java nicht verwenden, bearbeiten Sie die Dateien `/opt/IBM/ISP/mgmt/scripts/CommandEngine.sh` und `/opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh` auf dem Verwaltungsserver. Ändern Sie den Wert `export JAVA_HOME=` in jeder Datei, um auf die Java JRE-Position auf dem Server zu verweisen.

Nächste Schritte

Stellen Sie sicher, dass das Plattformsteuerungstool ordnungsgemäß installiert wurde, indem Sie Services mithilfe des Plattformsteuerungstool starten, stoppen und abfragen.

Zugehörige Konzepte:

„Installation mit Topologiedateien" auf Seite 39
IBM Intelligent Operations Center wird mithilfe einer Topologiedatei installiert. Die Topologiedatei ist eine XML-Datei, die die Parameter und Werte definiert, die beim Einsatz von IBM Intelligent Operations Center über verschiedene Server verwendet werden. Darüber hinaus definiert die Topologiedatei die zur Implementierung von Komponenten verwendete Sequenz.

Zugehörige Tasks:

„Services starten" auf Seite 206
Zum Starten von Services, die auf IBM Intelligent Operations Center-Servern ausgeführt werden, ist das Plattformsteuerungstool verfügbar.

„Services stoppen" auf Seite 209
Zum Stoppen von IBM Intelligent Operations Center-Services ist das Plattformsteuerungstool verfügbar.

„Status der Services abfragen" auf Seite 212
Das Plattformsteuerungstool ist für die Bestimmung des Status von IBM Intelligent Operations Center-Services verfügbar.

Das Tool Systemprüfung installieren

Das Tool Systemprüfung wird verwendet, um den Betriebsstatus von Komponenten in IBM Intelligent Operations Center zu überprüfen. Das Tool wird getrennt vom Produkt installiert.

Vorbereitende Schritte

Das Produkt IBM Intelligent Operations Center muss bereits vor Installation des Tools Systemprüfung installiert sein.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

1. Öffnen Sie auf dem Installationsserver ein Terminalfenster und melden Sie sich als `root` an. Sind Sie nicht als `root` angemeldet, wechseln Sie mit dem Befehl **`su -`** zum `root`-Account.
2. Führen Sie den Befehl **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`** aus.
3. Wechseln Sie in das Verzeichnis *`Installationsausgangsverzeichnis`*`/cat/bin`.
4. Führen Sie den Befehl **`./install-cat-lite.sh -d`***Installationsausgangsverzeichnis*`/cat -f` *Installationsausgangsverzeichnis*`/ioc/topology/iop_lite_topo.properties -p` *Kennwort* aus. Dabei ist *Kennwort* das Topologiekennwort.

   Anmerkung: Der Befehl muss vom Verzeichnis *`Installationsausgangsverzeichnis`*`/cat/bin` aus ausgeführt werden.
   Das Tool Systemprüfung ist erfolgreich installiert, wenn für alle installierten Komponenten der Status `[ OK ]` angezeigt wird.
5. Starten Sie alle IBM Intelligent Operations Center-Server neu.
   a. Fahren Sie alle IBM Intelligent Operations Center-Server mithilfe des Plattformsteuerungstools herunter.
   b. Fahren Sie alle Server herunter und starten Sie sie über das Betriebssystem neu.
   c. Starten Sie alle IBM Intelligent Operations Center-Server mithilfe des Plattformsteuerungstools.

Nächste Schritte

Überprüfen Sie, ob das Tool Systemprüfung ordnungsgemäß installiert wurde, indem Sie das Tool Systemprüfung ausführen.

Zugehörige Tasks:

„Verwendung des Systemprüfungtools" auf Seite 220
Das Systemprüfungstool wird zum Ermitteln des Betriebsstatus von Services verwendet, aus denen sich das IBM Intelligent Operations Center-System zusammensetzt.

„Services stoppen" auf Seite 209
Zum Stoppen von IBM Intelligent Operations Center-Services ist das Plattformsteuerungstool verfügbar.

„Services starten" auf Seite 206
Zum Starten von Services, die auf IBM Intelligent Operations Center-Servern ausgeführt werden, ist das Plattformsteuerungstool verfügbar.

IBM Intelligent Operations Center-Anwendung installieren

Installieren Sie die IBM Intelligent Operations Center-Anwendung nach der Installation der IBM Intelligent Operations Center-Architektur einschließlich Systemprüfung und Plattformsteuerungstool.

Vorbereitende Schritte

Die IBM Intelligent Operations Center-Architektur muss installiert sein und alle Services müssen gestartet werden.

Vorgehensweise

1. Öffnen Sie auf dem Installationsserver ein Terminalfenster und melden Sie sich als `root` an. Sind Sie nicht als `root` angemeldet, wechseln Sie mit dem Befehl **`su -`** zum `root`-Account.
2. Führen Sie den Befehl **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`** aus.
3. Wechseln Sie in das Verzeichnis *`Installationsausgangsverzeichnis`*`/ioc`.
4. Führen Sie den Befehl **`cp topology/iop_lite_topo.xml topology/iop_lite_topo_phase2.xml`** aus.
5. Führen Sie den Befehl **`bin/ba.sh installTopology -t ioc_lite_topo -p`** *Kennwort* aus. Dabei ist *Kennwort* das Topologiekennwort. Die Installation installiert die IBM Intelligent Operations Center-Anwendung. Dieser Schritt kann bis zu einer Stunde dauern.

   Es werden Nachrichten angezeigt, die Aufschluss über den Installationsfortschritt geben. In diesen Nachrichten wird der Status der installierten Komponente angegeben. Folgende Statusangaben sind möglich:

   [OK] Die Komponente wurde erfolgreich installiert.

   [Fail] (fehlgeschlagen)
   Die Installation der Komponente ist fehlgeschlagen.

Ergebnisse

Die IBM Intelligent Operations Center-Anwendung ist erfolgreich installiert, wenn alle Nachrichten mit dem Status `[ OK ]` abschließen.

Installation überprüfen

Überprüfen Sie nach der Installation von IBM Intelligent Operations Center dass das Produkt ordnungsgemäß installiert wurde.

Vorgehensweise

Starten Sie alle Services.

1. Starten Sie alle IBM Intelligent Operations Center-Services durch Ausführung des Plattformsteuerungstool mit dem Parameter **start all**.
2. Überprüfen Sie durch Prüfung der angezeigten Nachrichten, dass alle Services erfolgreich gestartet wurden.
3. Führen Sie alle Tests im Systemprüfung-Tool durch.
4. Überprüfen Sie, dass alle Tests erfolgreich ausgeführt wurden.

Optional können Sie alle Services abschalten und erneut starten.

5. Stoppen Sie alle IBM Intelligent Operations Center-Services durch Ausführung des Plattformsteuerungstool mit dem Parameter **stop all**.
6. Überprüfen Sie anhand der angezeigten Nachrichten, ob alle Services erfolgreich gestoppt wurden.
7. Schalten Sie das Betriebssystem Linux auf allen Servern ab.
8. Schalten Sie alle Laufzeitserver aus und wieder ein oder führen Sie für alle Server einen Warmstart durch.
9. Starten Sie alle IBM Intelligent Operations Center-Services durch Ausführung des Plattformsteuerungstool mit dem Parameter **start all**.
10. Überprüfen Sie durch Prüfung der angezeigten Nachrichten, dass alle Services erfolgreich gestartet wurden.
11. Führen Sie alle Tests im Systemprüfung-Tool durch.
12. Überprüfen Sie, dass alle Tests erfolgreich ausgeführt wurden.

Nächste Schritte

Wenn Fehler auftreten sollten, beheben Sie die Fehler und führen Sie diese Schritte erneut aus.

Zugehörige Konzepte:

„Produktinformationen” auf Seite 205
Im Portlet "Produktinformationen" können Sie Details zur Version des IBM Intelligent Operations Center und zur Version der integrierten IBM Smarter Cities Software Solutions anzeigen, die Sie installiert haben. Außerdem können Sie Details zu allen Aktualisierungen anzeigen, die Sie seit der Installation ausgeführt haben.

Zugehörige Tasks:

„Services starten” auf Seite 206
Zum Starten von Services, die auf IBM Intelligent Operations Center-Servern ausgeführt werden, ist das Plattformsteuerungstool verfügbar.

„IBM Intelligent Operations Center mithilfe des Installation Managers installieren” auf Seite 28
IBM Intelligent Operations Center kann mithilfe des bereitgestellten grafisch orientierten Installationsprogramms installiert werden.

„Services stoppen” auf Seite 209
Zum Stoppen von IBM Intelligent Operations Center-Services ist das Plattformsteuerungstool verfügbar.

„Verwendung des Systemprüfungtools” auf Seite 220
Das Systemprüfungstool wird zum Ermitteln des Betriebsstatus von Services verwendet, aus denen sich das IBM Intelligent Operations Center-System zusammensetzt.

Konfiguration nach der Installation von IBM Intelligent Operations Center

Nach der schrittweise oder mithilfe des Installation Managers durchgeführten Installation der IBM Intelligent Operations Center-Architektur sind mehrere Schritte der Konfiguration nach der Installation erforderlich, um die Installation abzuschließen.

Wichtig: Alle Arbeiten der Konfiguration nach der Installation müssen abgeschlossen sein, bevor Cyber Hygiene installiert wird.

Zugehörige Tasks:

„IBM Intelligent Operations Center mithilfe des Installation Managers installieren" auf Seite 28
IBM Intelligent Operations Center kann mithilfe des bereitgestellten grafisch orientierten Installationsprogramms installiert werden.

Services für Zusammenarbeit für IPv6 konfigurieren

Wenn Ihre Installation Netzbetrieb mit IPv6 verwendet, sind für Services für Zusammenarbeit Konfigurationsschritte erforderlich.

Informationen zu diesem Vorgang

Die IBM Intelligent Operations Center-Architektur muss installiert sein, bevor der Netzbetrieb mit IPv6 für Services für Zusammenarbeit konfiguriert wird.

Vorgehensweise

1. Folgen Sie den Schritten in der Dokumentation für Lotus Domino, um Lotus Domino für die IPv6-Adressierung zu konfigurieren.
2. Folgen Sie den Schritten in der Dokumentation für Lotus Sametime Standard, um Lotus Sametime Standard für die IPv6-Adressierung zu konfigurieren.
3. Folgen Sie den Schritten in der Dokumentation für WebSphere Portal, um zu konfigurieren, was beim Portlet 'Sametime Contact List' als vertrauenswürdig anerkannt wird, falls Sie kein IPv4-Netz mit einer IPv4-Adresse verwenden, die dem Ereignisserver zugeordnet ist.

Zugehörige Informationen:

Lotus Domino für die IPv6-Adressierung konfigurieren

Den Sametime Community-Server zur Unterstützung von IPv6 konfigurieren

Konfigurieren, was beim Portlet 'Sametime Contact List' als vertrauenswürdig anerkannt wird

Single Sign-on für Services zur Zusammenarbeit konfigurieren

Importieren Sie das WebSphere Portal SSO LTPA-Token in den Ereignisserver, um es Benutzern zu ermöglichen, auf die Services zur Zusammenarbeit zuzugreifen, ohne dass sie ihre Identifikationsdaten erneut eingeben müssen.

Informationen zu diesem Vorgang

Die Architektur von IBM Intelligent Operations Center muss installiert werden, bevor das LTPA-Token (Lightweight Third-Party Authentication) importiert wird.

Dieses Token wurde während der Installation der Architektur von IBM Intelligent Operations Center erstellt.

Vorgehensweise

1. Installieren Sie einen Lotus Notes 8.5.x Client auf einer Workstation. Es kann eine vorhandene Installation verwendet werden. Die Workstation muss unter Verwendung des vollständig qualifizierten Hostnamens über TCP/IP eine Verbindung zum Ereignisserver herstellen können.
2. Kopieren Sie die Datei `/opt/pdweb/etc/stproxy.ltpa` vom Anwendungsserver auf die Workstation, die Lotus Notes ausführt. Dies ist das LTPA-Token, das in das Verzeichnis für Services zur Zusammenarbeit importiert wird.
3. Kopieren Sie die Datei `/local/notesdata/admin.id` vom Ereignisserver auf die Workstation, die Lotus Notes ausführt. Dies ist die ID-Datei für den Administrator für Services zur Zusammenarbeit. Sie verwenden diese Kennung, um sich im Verzeichnis für Services zur Zusammenarbeit anzumelden.

4. Starten Sie auf der Workstation den Lotus Notes Client und melden Sie sich mit der Datei `admin.id` an.
   a. Klicken Sie im Anmeldefenster von Lotus Notes auf **Benutzername**.
   b. Navigieren Sie zu dem Verzeichnis, in das Sie die Datei `admin.id` kopiert haben, und wählen Sie sie aus.
   c. Geben Sie das Kennwort ein, das in der Datei mit den Topologieeigenschaften für die Eigenschaft `DOMINO.ADMIN.PWD` festgelegt ist.
   d. Wenn eine Sicherheitswarnung angezeigt wird, klicken Sie auf **Ja**.
5. Öffnen Sie die Datei `names.nsf`.
   a. Klicken Sie auf **Datei** > **Öffnen** > **Lotus Notes-Anwendung**.
   b. Geben Sie den vollständig qualifizierten Hostnamen des Ereignisserver in **Suchen in** ein.
   c. Geben Sie `names.nsf` in **Dateiname** ein.
   d. Klicken Sie auf **Öffnen**.
6. Navigieren Sie zu **Web** > **Webkonfigurationen**.
7. Wählen Sie `SSO-Webkonfiguration für LTPA-Token` aus und klicken Sie auf **Dokument bearbeiten**.
8. Klicken Sie auf **Schlüssel** > **WebSphere LTPA-Schlüssel importieren**. Klicken Sie auf **OK**, wenn Sie eine Warnung zum Überschreiben vorhandener Schlüssel erhalten.
9. Geben Sie den Pfad zu der Position ein, in die die Datei `stproxy.ltpa` kopiert wurde. Klicken Sie auf **OK**.
10. Geben Sie das Kennwort für das LTPA-Token ein. Das Kennwort ist in der Eigenschaft `WAS.LTPA.PWD` der Datei mit den Topologieeigenschaften definiert.
11. Klicken Sie auf **OK** > **Speichern und schließen**.
12. Starten Sie den Service für Zusammenarbeit mithilfe des Plattformsteuerungstool neu.
    a. Melden Sie sich am Verwaltungsserver an, und öffnen Sie ein Terminalfenster.
    b. Führen Sie **`su -ibmadmin`** aus.
    c. Führen Sie **`/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop st`** *Kennwort* aus, wobei *Kennwort* das Kennwort für das Plattformsteuerungstool ist, das bei der Installation des Plattformsteuerungstool festgelegt wurde.
    d. Führen Sie **`/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start st`** *Kennwort* aus, wobei *Kennwort* das Kennwort für das Plattformsteuerungstool ist, das bei der Installation des Plattformsteuerungstool festgelegt wurde.

Sitzungszeitlimit einstellen

Mit dem Sitzungszeitlimit wird die Dauer bestimmt, über die ein Benutzer inaktiv sein kann, bevor die Sitzung beendet wird und der Benutzer sich erneut anmelden muss. Das Sitzungszeitlimit betrifft auch Administratoren, die über den Portalservice angemeldet sind.

Informationen zu diesem Vorgang

Wenn IBM Intelligent Operations Center installiert ist, ist kein Sitzungszeitlimit definiert. Benutzer bleiben angemeldet, bis sie sich abmelden, auch wenn die Sitzung inaktiv ist.

Wenn in Ihrer Organisation Sicherheitsrichtlinien gelten, die erfordern, dass Sitzungen nach einem Inaktivitätszeitraum abgemeldet werden, führen Sie die folgenden Schritte aus, um ein Sitzungszeitlimit für Ihr IBM Intelligent Operations Center-System zu definieren.

Vorgehensweise

1. Gehen Sie mithilfe eines Web-Browsers zu `http://`*`Anwendungsserver`*`:9060/ibm/console`, wobei *Anwendungsserver* der Hostname des Anwendungsserver ist.

2. Melden Sie sich als Benutzer `waswebadmin` mit dem für `PORTAL.ADMIN.ACCOUNT.PWD` in der Datei mit den Topologieeigenschaften definierten Kennwort an.
3. Klicken Sie auf **Server** > **Servertyp** > **WebSphere Application-Server** > **WebSphere Portal**.
4. Klicken Sie auf **Containereinstellungen** > **Sitzungsmanagement** > **Zeitlimit festlegen**.
5. Geben Sie den gewünschten Wert für das Zeitlimit in Minuten ein.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Speichern**.
8. Klicken Sie auf **Server** > **Servertyp** > **WebSphere Application Server** > **STProxyServer1**.
9. Klicken Sie auf **Containereinstellungen** > **Sitzungsmanagement** > **Zeitlimit festlegen**.
10. Geben Sie den gewünschten Wert für das Zeitlimit in Minuten ein.
11. Klicken Sie auf **OK**.
12. Klicken Sie auf **Speichern**.
13. Klicken Sie auf **Server** > **Servertyp** > **WebSphere Application Server** > **CongnosX_GW1**.
14. Klicken Sie auf **Containereinstellungen** > **Sitzungsmanagement** > **Zeitlimit festlegen**.
15. Geben Sie den gewünschten Wert für das Zeitlimit in Minuten ein.
16. Klicken Sie auf **OK**.
17. Klicken Sie auf **Speichern**.
18. Klicken Sie auf **Server** > **Servertyp** > **WebSphere Application Server** > **CongnosX_Disp1**.
19. Klicken Sie auf **Containereinstellungen** > **Sitzungsmanagement** > **Zeitlimit festlegen**.
20. Geben Sie den gewünschten Wert für das Zeitlimit in Minuten ein.
21. Klicken Sie auf **OK**.
22. Klicken Sie auf **Speichern**.
23. Stoppen Sie den Anwendungsserver, und starten Sie ihn dann erneut.
24. Melden Sie sich auf dem Anwendungsserver als Benutzer `ibmadmin` mit dem für `IOP.ADMIN.USER.PWD` in der Datei mit den Topolgieeigenschaften definierten Kennwort an.
25. Führen Sie den Befehl **`sudo su -`** aus, um zum `root`-Benutzer zu wechseln.
26. Bearbeiten Sie die Datei `/opt/pdweb/etc/webseald-default.conf` mit einem Texteditor.
27. Ändern Sie im Abschnitt `SESSION CACHE SETTINGS` den Wert `timeout = 0` zu dem gewünschten Sitzungszeitlimit (in Sekunden). Das Zeitlimit muss mit der Zeit, die für den Portalservice eingestellt wurde, übereinstimmen. Allerdings wird der Wert für das Portal in Minuten eingestellt und die Cacheeinstellung für die Sitzung in Sekunden. Der Wert in den Cacheeinstellungen für Sitzungszeitlimits muss genau das 60-fache des Werts, der für den Portalservice eingestellt wurde, sein. Wenn z. B. der Portalwert 30 (Minuten) ist, muss der Wert der Cacheeinstellungen für Sitzungen bei 1800 (Sekunden) liegen.
28. Führen Sie den Befehl **`/usr/bin/pdweb restart`** aus, um den Sicherheitsservice neu zu starten.

Semantic Model Services installieren und konfigurieren

IBM Intelligent Operations Center stellt eine Semantic Model Services-Anwendung und ein Beispielmodell bereit. Der Service muss vor der Verwendung installiert und konfiguriert sein.

Jazz Team Server konfigurieren

IBM Intelligent Operations Center Semantic Model Services ist auf einem Jazz Team Server installiert. Der Jazz Team Server muss konfiguriert sein, bevor die IBM Intelligent Operations Center Semantic Model Services installiert werden.

Informationen zu diesem Vorgang

Die IBM Intelligent Operations Center-Architektur muss installiert sein, bevor der Jazz Team Server konfiguriert wird.

Vorgehensweise

1. Gehen Sie in einem Web-Browser zu `http://management_host:82/jts/setup`, wobei *management_host* der vollständig qualifizierte Hostname des Verwaltungsserver ist.
2. Melden Sie sich mit der Benutzer-ID `iicsystemuser` und dem Kennwort `passw0rd` an.
3. Klicken Sie auf **Next** (Weiter).
4. Auf der Seite "Configure Public URI" (Öffentliche URI konfigurieren) geben Sie einen Wert für **Public URI Root** (Root der öffentlichen URI) in der Form `https://management_host:9448/jts` an und wählen Sie die Option `I understand that once the Public URI is set, it cannot be modified` (Ich verstehe, dass eine einmal festgelegte öffentliche URI nicht mehr geändert werden kann) an. Klicken Sie auf **Next** (Weiter).
5. Klicken Sie auf die Option zum Testen der Verbindung. Es sollte eine Nachricht angezeigt werden, die darüber informiert, dass der Konfigurationstest erfolgreich war.
6. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu speichern und fortzufahren.
7. Konfigurieren Sie die Datenbank auf der Seite "Configure Database" (Datenbank konfigurieren).
   a. Wählen Sie `DB2` für **Database Vendor** (Datenbankanbieter) aus.
   b. Wählen Sie `JDBC` für **Connection Type** (Verbindungstyp) aus.
   c. Geben Sie das DB2-Datenbankkennwort, das in der Datei mit den Topologieeigenschaften als Eigenschaft `DEFAULT.PWD.DB2` definiert ist, für **JDBC password** (JDBC-Kennwort) ein. Ignorieren Sie die angezeigte Kennwortnachricht.
   d. Geben Sie für **JDBC location** (JDBC-Position) `//db_host:50005/JTS:user=db2inst5;password={password};` ein, wobei *db_host* der Hostname des Datenserver ist. Die Zeichenfolge {password} muss wie dargestellt werden wie angezeigt. Ersetzen Sie sie nicht mit einem Kennwortwert.
   e. Klicken Sie auf die Option zum Testen der Verbindung. Tritt ein Fehler auf, überprüfen und korrigieren Sie die Einträge. Wenn die Einträge korrekt sind, stellen Sie sicher, dass die Datenbankservices auf dem Datenserver mithilfe des Plattformsteuerungstool gestartet wurden.
   f. Klicken Sie auf **Create Tables** (Tabellen erstellen), nachdem eine Nachricht angezeigt wurde, dass in der Datenbank keine Jazz-Tabellen vorhanden sind. Die Verarbeitung dauert mehrere Minuten.
   g. Klicken Sie auf **Next** (Weiter).
8. Setzen Sie auf der Seite "Enable E-mail Notification" (E-Mail-Benachrichtigung aktivieren) den Wert auf **Disabled** (Inaktiviert) und klicken Sie auf **Next** (Weiter).
9. Auf der Seite "Register Applications" (Anwendungen registrieren) sollte die Nachricht "No new applications detected" (Keine neuen Anwendungen gefunden) angezeigt werden. Klicken Sie auf **Next** (Weiter).
10. Wählen Sie **LDAP** für **User Registry Type** (Benutzerregistertyp) in Schritt 1 auf der Seite zum Einrichten des Benutzerregisters aus.
11. Konfigurieren Sie in Schritt 2 LDAP für das Register von Jazz Team Server.
    a. Geben Sie `ldap://mgmt_host:389` für **LDAP Registry Location** (LDAP-Registerposition) ein, wobei *mgmt_host* der vollständig qualifizierte Hostname des Verwaltungsserver ist.
    b. Geben Sie `OU=USERS,OU=SWG,O=IBM,C=US` für **Base User DN** (Basisbenutzer-DN) ein.
    c. Geben Sie `userId=uid,name=cn,emailAddress=mail` für **User Property Names Mapping** (Zuordnung von Benutzereigenschaftsnamen) ein.
    d. Geben Sie `OU=GROUPS,OU=SWG,O=IBM,C=US` für **Base Group DN** ein.
    e. Stellen Sie bei **Jazz to LDAP Group Mapping** (Zuordnung von Jazz- zu LDAP-Gruppen) sicher, dass der Wert auf `JazzAdmins=JazzAdmins, JazzUsers=JazzUsers, JazzDWAdmins=JazzDWAdmins, JazzProjectAdmins=JazzProjectAdmins, JazzGuests=JazzGuests` gesetzt ist.
    f. Geben Sie `cn` für **Group Name Property** (Gruppennamenseigenschaft) ein.
    g. Geben Sie `cn` für **Group Member Property** (Gruppenmitgliedseigenschaft) ein.

12. Klicken Sie auf die Option zum Testen der Verbindung. Wenn eine Warnung angezeigt wird, klicken Sie auf **show details**. Wenn die Warnung sich auf die Eigenschaft `mail` bezieht, können Sie die Nachricht ignorieren.
13. Wählen Sie `IBM Integrated Information Core - IIC Model Server` für **Client Access License Type** (Lizenztyp für Clientzugriff) aus.
14. Klicken Sie auf **Next** (Weiter).
15. Wählen Sie für **Configure Data Warehouse** (Data-Warehouse konfigurieren) das Kontrollkästchen `I do not wish to configure the data warehouse at this time` (Ich möchte das Data-Warehouse im Moment nicht konfigurieren) aus.
16. Klicken Sie auf der Übersichtsseite auf **Finish** (Fertigstellen).

Ergebnisse

Der Jazz Team Server ist betriebsbereit.

Semantic Model Services installieren

Die Semantic Model Services und eine Beispielanwendung werden gemeinsam mit IBM Intelligent Operations Center zur Verfügung gestellt.

Informationen zu diesem Vorgang

Die Konfiguration des Jazz Team Servers auf dem Verwaltungsserver ist erforderlich, bevor die Semantic Model Services verwendet werden.

Vorgehensweise

1. Gehen Sie in einem Web-Browser zu `http://`*`management_host`*`:82/jts/admin`, wo *management_host* der vollständig qualifizierte Hostname des Verwaltungsserver ist.
2. Auf der Serveradministrationsseite klicken Sie auf **Server** > **Konfiguration** > **Anwendungen eintragen**.
3. Klicken Sie auf **Hinzufügen** auf der Seite "Eingetragene Anwendungen".
4. Fügen Sie auf der Seite "Anwendung hinzufügen" die Modellserveranwendung hinzu.
   a. Geben Sie `Model Server` als **Anwendungsname** ein.
   b. Geben Sie `http://`*`management_host`*`:82/modelserver/scr` ein, wobei *management_host* der vollständig qualifizierte Hostname des Verwaltungsserver für **Erkennungs-URL** ist.
   c. Geben Sie für **Konsumentengeheimnis** einen Wert Ihrer Wahl ein. Dieser Wert wird dann verwendet, um Zugang zu der Anwendung zu geben. Der Wert sollte mit derselben Sicherheit behandelt werden wie ein Kennwort.
   d. Geben Sie `iicsystemuser` als **Funktions-ID** ein.

   Der **Anwendungstyp** wird zu `Modell Server` geändert.
5. Wenn es keine Fehlernachrichten gibt, klicken Sie auf **fertigstellen**.

Die Konfiguration von Semantic Model Services überprüfen

Eine Beispielanwendung der Semantic Model Services wird gemeinsam mit dem IBM Intelligent Operations Center bereitgestellt und kann verwendet werden, um die ordnungsgemäße Installation und Konfiguration der Semantic Model Services zu überprüfen.

Vorgehensweise

1. Bereiten Sie die Beispielmodelldateien vor.
   a. Suchen Sie auf dem Installationsserver die Datei `iic15_2_stagebuildtoserver.xx.jar` im Verzeichnis *`install_media`*.
   b. Fügen Sie die Datei `iic15_2_stagebuildtoserver.xx.jar` in ein Verzeichnis Ihrer Wahl ein. In der weiteren Beschreibung dieser Schritte wird auf dieses Verzeichnis als *model_home* verwiesen.

2. Installieren Sie das Beispielmodell.
   a. In einem Web-Browser auf dem Server, wo sich *model_home* befindet, gehen Sie zu `http://mgmt_host:82/iic/console`, wobei *mgmt_host* der vollständig qualifizierte Hostname des Verwaltungsserver ist.
   b. Melden Sie sich als Benutzer `iicsystemuser` mit dem Kennwort `passw0rd` an.
   c. Klicken Sie auf **Modellmanager** > **Ontologien** > **Durchsuchen**.
   d. Navigieren Sie zum Verzeichnis *install_media*`/ioc/image/IIC/install/modelServices/post_install/`.
   e. Öffnen Sie die Datei `rsm.owl`.
   f. Klicken Sie auf **Laden**. Die Datei wird geladen.
   g. Klicken Sie auf **Modellmanager** > **Ontologien** > **Durchsuchen**.
   h. Navigieren Sie zum Verzeichnis *install_media*`/ioc/image/IIC/install/modelServices/post_install/`.
   i. Öffnen Sie die Datei `modelServer.owl`.
   j. Klicken Sie auf **Laden**. Die Datei wird geladen.
   k. Klicken Sie auf **Modellmanager** > **Ontologien** > **Durchsuchen**.
   l. Navigieren Sie zum Verzeichnis *install_media*`/ioc/image/IIC/install/ktpRuntimeServices/post_install/`.
   m. Öffnen Sie die Datei `kpi.owl`.
   n. Klicken Sie auf **Laden**. Die Datei wird geladen.
   o. Klicken Sie auf **Modellmanager** > **Laden** > **Durchsuchen**
   p. Navigieren Sie zum Verzeichnis *install_media*`/ioc/image/IIC/samples/rdf/rsm/`.
   q. Öffnen Sie die Datei `IBMOilDownstreamSampleRDF.xml`.
   r. Klicken Sie auf **Laden**. Die Datei wird geladen.
   s. Klicken Sie auf **Modellmanager** > **Laden** > **Durchsuchen**
   t. Navigieren Sie zum Verzeichnis *install_media*`/ioc/image/IIC/samples/rdf/rsm/`.
   u. Öffnen Sie die Datei `IBMOilUpstreamSampleRDF.xml`.
   v. Klicken Sie auf **Laden**. Die Datei wird geladen.
   w. Klicken Sie auf **Modellmanager** > **Laden** > **Durchsuchen**
   x. Navigieren Sie zum Verzeichnis *install_media*`/ioc/image/IIC/samples/rdf/rsm/`.
   y. Öffnen Sie die Datei `IBMOilDownstreamSampleReferenceRDF.xml`.
   z. Klicken Sie auf **Laden**. Die Datei wird geladen.
   aa. Klicken Sie auf **Modellmanager** > **Laden** > **Durchsuchen**
   ab. Navigieren Sie zum Verzeichnis *install_media*`/ioc/image/IIC/samples/rdf/rsm/`.
   ac. Öffnen Sie die Datei `IBMOilUpstreamSampleReferenceRDF.xml`.
   ad. Klicken Sie auf **Laden**. Die Datei wird geladen.
3. Stellen Sie sicher, dass das Beispielmodell ordnungsgemäß installiert ist.
   a. Klicken Sie auf **Modellmanager** > **Abfrage** > **Abfrage**. Eine vordefinierte Abfrage wird ausgeführt. Eine XML-Struktur wird gemeinsam mit den Abfrageergebnissen angezeigt. Der Tag der höchsten Ebene sollte `spargl` sein und über die sekundären Tags `head` und `results` verfügen.
   b. Klicken Sie auf **Modellexplorer** und stellen Sie sicher, dass Sie das Modell durchsuchen können.
4. Verwenden Sie das Modell, um die Installation von Modellmanager zu prüfen.
   a. In einem Web-Browser auf dem Verwaltungsserver gehen Sie zu `http://mgmt_host:82/iic/ibmoil`, wobei *mgmt_host* der vollständig qualifizierte Hostname des Verwaltungsserver ist.
   b. Klicken Sie auf **IBM Oil Company** > **Variablen**. Web-Service-URLs werden angezeigt.

Ergebnisse

Die Semantic Model Services und das Beispielmodell IBM Oil wurden installiert.

Leistung von Semantic Model Services verbessern

Konfigurieren Sie die Semantic Model Services, die von IBM Intelligent Operations Center bereitgestellt werden, um die Leistung zu verbessern, wenn Abfragen von Modellen durchgeführt werden.

Vorgehensweise

1. Gehen Sie in einem Web-Browser zu `http://management_host:82/iic/console`, wobei *management_host* der vollständig qualifizierte Hostname des Verwaltungsserver ist.
2. Fügen Sie die Eigenschaftswerte in Tabelle 20 zu der Kategorie **OPCWEBSERVICE** hinzu.

Tabelle 20. Eigenschaften in OPCWEBSERVICE

Eigenschaft	Wert
cache.browse.timetolive.second	3600
cache.timetolive.second	2592000
cache.wait.second.after.create.action	1

3. Aktualisieren Sie die folgenden Eigenschaften und Werte und fügen Sie sie zu Tabelle 21 in der Kategorie RSM hinzu.

Tabelle 21. Eigenschaften von RSM

Eigenschaft	Wert
mvmViewPath.0	http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity##iec.ch/TC57/CIMgeneric# ISA95_Site##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.ManagedBy_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.has_measurement##http:// iec.ch/TC57/CIMgeneric#RSM_Measurement##http:// iec.ch/TC57/CIMgeneric# RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIMgeneric#RSM_MeasurementValue
mvmViewPath.1	http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity##iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http://iec.ch/TC57/CIMgeneric# ISA95_WorkCenter.Contains_Equipment##http:// iec.ch/TC57/CIMgeneric# RSM_WorkEquipment##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.has_measurement##http:// iec.ch/TC57/CIMgeneric#RSM_Measurement##http:// iec.ch/TC57/CIMgeneric# RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIMgeneric#RSM_MeasurementValue
mvmDownLevelPreRequest	3
mvmCacheProperty.0	cim:RSM_IdentifiedObject.name
mvmMaxQueryURI	500
mvmMaxSparqlEntry	4000

4. Klicken Sie auf **Veröffentlichen**. Die neuen und geänderten Eigenschaften werden gespeichert.

5. Starten Sie die Semantic Model Services mithilfe des Plattformsteuerungstool neu.
6. Gehen Sie in einem Web-Browser zu `http://management_host:82/iic/console`, wo *management_host* der vollständig qualifizierte Hostname des Verwaltungsserver ist.
7. Nehmen Sie die ggf. erforderlichen lösungs- oder anwendungsspezifischen Änderungen vor. Wenn Änderungen erforderlich sind, sind sie in der Dokumentation zum Produkt oder zur Lösung dokumentiert.

Das Plattformsteuerungstool konfigurieren

Nach der Installation von IBM Intelligent Operations Center müssen Sie, sofern Sie eine andere Java JRE installiert haben als die mit IBM Intelligent Operations Center bereitgestellte, die JRE-Position definieren, die vom Plattformsteuerungstool verwendet wird.

Vorgehensweise

1. Bearbeiten Sie auf dem Verwaltungsserver die Datei `/opt/IBM/ISP/mgmt/scripts/CommandEngine.sh`.
2. Verschieben Sie `export JAVA_HOME=` zu der Position der Java JRE.
3. Speichern Sie die Änderungen.
4. Bearbeiten Sie auf dem Verwaltungsserver die Datei `/opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh`.
5. Verschieben Sie `export JAVA_HOME=` zu der Position, der Java JRE.
6. Speichern Sie die Änderungen.

Zugehörige Tasks:

„Die Java-Laufzeitumgebung installieren” auf Seite 28
Die Java 6 Runtime-Umgebung muss auf dem Installationsserver installiert sein, bevor IBM Intelligent Operations Center installiert wird.

Das Verwaltungskennwort von Tivoli Service Request Manager verschlüsseln

Verwenden Sie die folgende Prozedur, um das Verwaltungskennwort von Tivoli Service Request Manager in Tivoli Netcool/Impact zu verschlüsseln.

Vorgehensweise

1. Melden Sie sich bei der Tivoli Netcool/Impact-Verwaltungskonsole unter `http://Ereignishost:9080/nci/main` an. Dabei ist *Ereignishost* der Name des Ereignisserver. Melden Sie sich als Benutzer `admin` mit dem Kennwort `netcool` an.
2. Klicken Sie auf **IOC Project** (IOC-Projekt).
3. Doppelklicken Sie im Abschnitt "Richtlinien" auf die Richtlinie **IOC_Sample_Password_Encoder**. Die Richtlinie wird im Fenster **Richtlinieneditor** geöffnet.
4. Geben Sie im Feld **Kennwort hier eingeben** das Kennwort für `Maxadmin` ein. Das Kennwort `Maxadmin` ist das Kennwort für Benutzer mit Verwaltungsaufgaben, das Sie während der Installation eingegeben haben.
5. Um die Richtlinie zu speichern, klicken Sie auf **Speichern**.
6. Klicken Sie auf das Symbol **Trigger Policy** (Richtlinie auslösen).
7. Klicken Sie auf **Ausführen**.
8. Blättern Sie im Abschnitt "Servicestatus" zu **PolicyLogger**, klicken Sie auf **View log for PolicyLogger** (Protokoll für PolicyLogger anzeigen) (Symbol mit dem Abwärtspfeil).
9. Suchen Sie im Fenster für die Richtlinienprotokollfunktion (Policy Logger) die Anweisung, die der folgenden Anweisung entspricht:

   ```
   11 May 2012 14:19:12,260: [IOC_Sample_Password_Encoder][pool-1-thread-46]Parser log: {aes}FF877B74ADF4DF1C2002F94ACB38FAFF
   ```

10. Kopieren Sie das verschlüsselte Kennwort **`Maxadmin`** aus der Anweisung. Beispiel:

    ```
    {aes}FF877B74ADF4DF1C2002F94ACB38FAFF
    ```

11. Doppelklicken Sie auf der Tivoli Netcool/Impact-Verwaltungskonsole im Abschnitt "Richtlinien" auf die Richtlinie **UTILS_LIBRARY_IOC_TSRM**. Die Richtlinie wird im Fenster **Richtlinieneditor** geöffnet.
12. Ersetzen Sie den Wert von *MAXAdminPassword* durch den verschlüsselten Wert, den Sie in Schritt 10 kopiert haben:

    ```
    MAXAdminPassword = "{aes}FF877B74ADF4DF1C2002F94ACB38FAFF";
    ```
13. Um die Richtlinie zu speichern, klicken Sie auf **Speichern**.
14. Klicken Sie auf **IOC Project** (IOC-Projekt).
15. Doppelklicken Sie im Abschnitt "Richtlinien" auf die Richtlinie **IOC_Sample_Password_Encoder**. Die Richtlinie wird im Fenster **Richtlinieneditor** geöffnet.
16. Löschen Sie im Feld **Kennwort hier eingeben** das Kennwort für **Maxadmin**.
17. Um die Richtlinie zu speichern, klicken Sie auf **Speichern**.

Mindestanzahl der Threads für den Ereignisprozessor festlegen

Die Mindestanzahl der Threads für den Ereignisprozessor muss aus Leistungsgründen auf 25 gesetzt werden.

Vorgehensweise

1. Melden Sie sich bei der Tivoli Netcool/Impact-Verwaltungskonsole unter `http://Ereignishost:9080/nci/main` an. Dabei ist *Ereignishost* der Name des Ereignisserver.
2. Klicken Sie auf **Service Status** > **EventProcessor** (Servicestatus > Ereignisprozessor).
3. Geben Sie `25` für **Minimum Number of Threads** (Mindestanzahl der Threads an).

   Anmerkung: Der Wert für **Minimum Number of Threads** (Mindestanzahl der Threads) kann nicht größer sein als der Wert für **Maximum Number of Threads** (Maximale Anzahl der Threads).
4. Klicken Sie auf **OK**.
5. Klicken Sie auf das Symbol zum Stoppen des Prozesses, um den Ereignisprozessor zu stoppen.
6. Klicken Sie auf das Symbol zum Starten des Prozesses, um den Ereignisprozessor zu starten.

Die Poolgröße des Standardthreads und des WebContainer-Threads ändern

Die Einstellungen für die Poolgröße der Threads `Default` und `WebContainer` müssen geändert werden, um die Leistung der Standard Operating Procedures zu optimieren.

Vorgehensweise

1. Klicken Sie auf dem Ereignisserver in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Administration Tools** > **Administration Consoles** (Intelligent Operations > Verwaltungstools > Verwaltungskonsolen).
2. Klicken Sie unter "Event Server" (Ereignisserver) auf **Standard Operating Procedure Application Server** (Anwendungsserver für Standard Operating Procedures).
3. Melden Sie sich als Administrator beim WebSphere Application Server an. Die Benutzer-ID wurde in der Eigenschaft `WAS.ADMIN.ACCOUNT` definiert und das Kennwort wurde in der Eigenschaft `WAS.ADMIN.ACCOUNT.PWD` in der Topologieeigenschaftendatei definiert, als das IBM Intelligent Operations Center installiert wurde.
4. Klicken Sie auf **Servers** > **Application servers** > **MXServer1** > **Thread Pools** > **WebContainer** (Server > Anwendungsserver > MXServer1 > Thread-Pools > WebContainer).
5. Geben Sie `50` für **Minimum Size** (Mindestgröße) ein.
6. Geben Sie `50` für **Maximum Size** (Maximale Größe) ein.
7. Klicken Sie auf **OK**.

8. Klicken Sie auf **Servers** > **Application servers** > **MXServer1** > **Thread Pools** > **Default** (Server > Anwendungsserver > MXServer1 > Thread-Pools > Default).
9. Geben Sie `20` für **Minimum Size** (Mindestgröße) ein.
10. Geben Sie `50` für **Maximum Size** (Maximale Größe) ein.
11. Klicken Sie auf **OK**.
12. Starten Sie den `TSRMCluster` neu.
    a. Klicken Sie auf **Server** > **Cluster**.
    b. Wählen Sie `TSRMCluster` aus.
    c. Klicken Sie auf **Stop** (Stoppen).
    d. Warten Sie, bis der Status auf rot wechselt.
    e. Klicken Sie auf **Start** (Starten).

Cyber Hygiene schrittweise installieren und ausführen

Cyber Hygiene wird getrennt von IBM Intelligent Operations Center installiert und ausgeführt und zwar erst, nachdem alle anderen Komponenten von IBM Intelligent Operations Center installiert, konfiguriert und aktiv sind. Cyber Hygiene ersetzt die Standardbetriebssystemkonfiguration durch eine Reihe sicherere Optionen, die die Sicherheitsbasis des IBM Intelligent Operations Center-Systems grundlegend verbessern.

Vorbereitende Schritte

Anmerkung: Cyber Hygiene wird innerhalb desselben Schrittes installiert und ausgeführt. Wenn Sie IBM Intelligent Operations Center mithilfe von IBM Installation Manager installieren, verwenden Sie diese Schritte nicht. Die Installation von IBM Installation Manager stellt eine Option zum Installieren und Ausführen von Cyber Hygiene zur Verfügung.

Hängen Sie alle Dateisysteme, die nicht bezüglich ihrer Sicherheit beurteilt werden sollen, ab, um die Zeit, die Cyber Hygiene für das Ausführen von Scans und Korrekturen benötigt, zu reduzieren. Beispielsweise können die Verzeichnisse *Installationsmedien* auf jedem Server nach Abschluss aller Installationsschritte gelöscht werden. Diese Verzeichnisse können vor dem Ausführen von Cyber Hygiene gelöscht oder abgehängt werden.

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Informationen zu diesem Vorgang

Das Ausführen von Cyber Hygiene sollte der letzte Schritt nach der Installation von IBM Intelligent Operations Center sein. Die Scans und Korrekturen werden im Hinblick auf Konfigurationssicherheitsrisiken ausgeführt, die infolge der Installation des Standardbetriebssystems und des Produkts IBM Intelligent Operations Center entstanden sind. Die ausgeführten Korrekturen wurden getestet, um zu bestätigen, dass IBM Intelligent Operations Center-Services ordnungsgemäß funktionieren.

Von Cyber Hygiene vorgenommene Änderungen am System können zu Problemen mit anderen Anwendungen und Lösungen führen. Beispielsweise stellen andere Anwendungen und Lösungen möglicherweise Anforderungen an die Linux-Umgebung, die der bewährten Sicherheitspraxis nicht entsprechen. Für die Installation oder Ausführung einer Anwendung oder Lösung ist es möglicherweise erforderlich, dass die Anmeldung an das System als `Root`-Benutzer erfolgt. In diesem Fall müssen manche der Änderungen von Cyber Hygiene temporär oder dauerhaft geändert werden oder vom Anbieter der Anwendung oder Lösung muss eine andere Lösungsmöglichkeit gefunden werden.

Sind Änderungen von Cyber Hygiene einmal vorgenommen, gibt es keine automatisierte Methode, sie zu ändern. Alle Änderungen müssen durch manuelle Aktualisierungen des Betriebssystems Linux oder durch Änderung der Datei- oder Verzeichnisberechtigungen erfolgen.

Vorgehensweise

1. Öffnen Sie auf dem Installationsserver ein Terminalfenster und melden Sie sich als `root` an. Sind Sie nicht als `root` angemeldet, wechseln Sie mit dem Befehl **`su -`** zum `root`-Account.
2. Führen Sie den Befehl **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`** aus. Die Variable `JAVA_HOME` ist auf Java Runtime Environment (JRE) eingestellt.
3. Wechseln Sie in das Verzeichnis *`Installationsausgangsverzeichnis`*`/ch/install`.
4. Bearbeiten Sie die Datei `iop-ch-install.xml` mithilfe eines Texteditors.
5. Ersetzen Sie die Parameter in der Datei `iop-ch-install.xml` mit den für Ihre Installation angemessenen Werten.

Tabelle 22. Installationsparameter von Cyber Hygiene

Parameter	Wert
`${APP.1.HOST}`	Der vollständig qualifizierte Hostname des Anwendungsserver
`${APP.1.ACCT}`	Der Linux-Benutzername für SSH-Zugriff auf den Anwendungsserver
`${APP.1.ACCT.PWD}`	Das Kennwort für `${APP.1.ACCT}`
`${APP.1.SSH_PORT}`	Der Anwendungsserver SSH-Port
`${DB.1.HOST}`	Der vollständig qualifizierte Hostname des Datenserver
`${DB.1.ACCT}`	Der Linux-Benutzername für SSH-Zugriff auf den Datenserver
`${DB.1.ACCT.PWD}`	Das Kennwort für `${DB.1.ACCT}`
`${DB.1.SSH_PORT}`	Der Datenserver SSH-Port
`${EVENT.1.HOST}`	Der vollständig qualifizierte Hostname des Ereignisserver
`${EVENT.1.ACCT}`	Der Linux-Benutzername für SSH-Zugriff auf den Ereignisserver
`${EVENT.1.ACCT.PWD}`	Das Kennwort für `${EVENT.1.ACCT}`
`${EVENT.1.SSH_PORT}`	Der Ereignisserver SSH-Port
`${MGMT.1.HOST}`	Der vollständig qualifizierte Hostname des Verwaltungsserver
`${MGMT.1.ACCT}`	Der Linux-Benutzername für SSH-Zugriff auf den Verwaltungsserver
`${MGMT.1.ACCT.PWD}`	Das Kennwort für `${MGMT.1.ACCT}`
`${MGMT.1.SSH_PORT}`	Der Verwaltungsserver SSH-Port

6. Speichern Sie die Datei.
7. Wechseln Sie in das Verzeichnis *`Installationsausgangsverzeichnis`*`/ch`.
8. Führen Sie den Befehl *Installationsausgangsverzeichnis***`/ch/install/iop-ch-install.sh -r iop-ch-install-messages.properties -f 'com.ibm.iop.cyber.hygiene.scripts.lite_1.5.0.zip' -d`** *Installationsmedien***`/ioc/image -p`** *GRUB-Kennwort* aus. Dabei ist *GRUB-Kennwort* das Kennwort für das GRUB-Bootladeprogramm auf den Servern. Das *GRUB_Kennwort* wird auf alle Zielserver angewendet. Normalerweise ist bei einem Neustart von Servern kein Kennwort erforderlich. Aber sobald Cyber Hygiene installiert ist, muss das *GRUB_Kennwort* auf der Serverkonsole eingegeben werden, wenn Sie einen Server mit einer Linux-Option starten, wie z. B. wenn Sie im Einzelbenutzermodus starten.

Ergebnisse

Die Verarbeitungszeit wird durch die Geschwindigkeit der Hardware bestimmt und länger, wenn sich unnötige Dateien auf den Zielservern befinden. Die Verarbeitung kann bis zu 90 Minuten dauern. In dieser Zeit werden Zielserver gescannt und die notwendigen Korrekturen ausgeführt.

Nächste Schritte

Überprüfen Sie das Protokoll von Cyber Hygiene auf Fehler. Die Protokolle zeigen außerdem die ausgeführten Korrekturen und die optionalen manuellen Schritte an.

Zugehörige Konzepte:

„Übersicht über Cyber Hygiene" auf Seite 87
Das IBM Intelligent Operations Center-Feature Cyber Hygiene stellt Services bereit, um gegen potenzielle Sicherheitsrisiken im installierten System vorzugehen.

Änderungen am Betriebssystem Linux

Cyber Hygiene scannt das Betriebssystem Linux nach anerkannten Sicherheitsrisiken und nimmt die entsprechenden Änderungen vor. Protokolle beschreiben die gescannten Risiken und vorgenommenen Veränderungen an Richtlinien und Einstellungen des Betriebssystems Linux.

Die Protokolle listen außerdem Risiken auf, die erkannt wurden, aufgrund derer aber keine Änderungen vorgenommen wurden. Dies können u. a. folgende sein:

- Das System ist bereits so konfiguriert, wie es sonst durch Cyber Hygiene geschehen wäre.
- Für die Änderung ist es erforderlich, dass ein Systemadministrator eine Maßnahme ergreift oder entscheidet, ob die Änderung der Umgebung angemessen ist.
- Die Änderung kann nicht von einem automatisierten Script vorgenommen werden. Dies ist z. B. der Fall, wenn das Sicherheitsrisiko sich auf die allgemeinen Sicherheitsrichtlinien der Organisation bezieht.

Alle von Cyber Hygiene vorgenommenen Korrekturen können bei Bedarf später geändert werden. Die Protokolle von Cyber Hygiene stellen Informationen zu am System vorgenommenen Änderungen bereit. Änderungen können erforderlich sein, um Systeme mit anderen Anwendungen oder Lösungen verwenden zu können, wenn die von Cyber Hygiene vorgenommenen Änderungen mit diesen Systemen inkompatibel sind.

Das Protokoll von Cyber Hygiene überprüfen

Nachdem Cyber Hygiene installiert ist und ausgeführt wurde, überprüfen Sie das Protokoll, um die am System vorgenommenen Änderungen und verbleibende Sicherheitsrisiken zu verstehen.

Informationen zu diesem Vorgang

Wechseln Sie auf dem Installationsserver in das Verzeichnis, in das das Installationspaket für IBM Intelligent Operations Center kopiert wurde. In diesen Schritten wird dieses Verzeichnis als *Installationsausgangsverzeichnis* bezeichnet.

Vorgehensweise

1. Überprüfen Sie das Protokoll von Cyber Hygiene im Verzeichnis `/var/ibm/InstallationManager/logs/native` auf dem Installationsserver auf Vollständigkeit, um sicherzustellen, dass alle Aktionen auf allen Servern ausgeführt wurden. Das Protokoll kann mithilfe des Befehls **`fgrep yber *.log`** ermittelt werden. Die Protokolldatei zeigt Informationen für jeden Server an. Im Allgemeinen umfassen Protokollinformationen die folgenden Schritte:
   - Vorbereitung der Umgebung auf die Ausführung der Tasks von Cyber Hygiene.

- Ausführen des eigenständigen Korrekturprogramms. Dieses behebt Risiken, die kein Scannen erfordern. Dazu gehören z. B. die Einstellung eines Kennwortes für das GRUB-Bootladeprogramm und das Einschalten der Protokollierung.
- Inaktivieren des fernen Root-Anmeldens.
- Scannen nach Sicherheitsrisiken. Dieses Scannen wird im Hintergrund ausgeführt und die Haupttask wartet auf den Abschluss des Scanvorgangs.
- Ausführen des Korrekturprogramms, um gegen während des Scanvorgangs entdeckte Sicherheitsrisiken vorzugehen.
- Scannen im Anschluss an die Korrektur. Dieses Scannen erkennt Risiken, die beim ersten Scannen nicht erkannt wurden.
- Ausführen des Korrekturprogramms, um gegen zusätzliche, beim zweiten Scan entdeckte Sicherheitsrisiken vorzugehen. Nicht abgeschlossene Korrekturen werden protokolliert.

2. Überprüfen Sie die detaillierten Protokolle von Cyber Hygiene, die sich im Verzeichnis `/var/BA15/CH/results` auf jedem Zielserver befinden. Das Protokoll `standrem-`*`Datum_Uhrzeit`*`.log` zeigt die Ergebnisse des eigenständigen Korrekturprogramms an. Das Protokoll `standrem-disableRemoteRoot-`*`Datum_Uhrzeit`*`.log` zeigt die Ergebnisse der Inaktivierung der fernen Root-Anmeldung an. Das Protokoll `scanrem-combined-log-`*`Datum_Uhrzeit`*`.log` zeigt die Ergebnisse der gescannten Aktionen des Korrekturprogramms an. Es gibt zwei Protokolle für die beiden Scan- und Korrekturschritte.
   a. Überprüfen Sie die Protokolldateien auf Zeilen, die mit dem Wort `Vulnerability` (Schwachstelle) beginnen. Jede Zeile gibt die durchgeführte Aktion an und umfasst Folgendes:
      - Die Untersuchungsergebnisse des Scans.
      - Die ausgewählten Korrekturen.
      - Die Details der angewendeten Korrekturen.
   b. Im Protokoll für den zweiten Scan und die zweite Korrektur müssen Korrekturen, die mit der Anmerkung `NOT DONE` versehen sind, möglicherweise auf zusätzliche manuelle Aktionen untersucht werden.

Ferne Rootanmeldung wieder aktivieren

Cyber Hygiene inaktiviert die ferne Anmeldung beim `root`-Account durch den Befehl **`ssh`**. Die Befehle **`telnet`** und **`rsh`** sind im Betriebssystem Linux vollständig inaktiviert. Die ferne Anmeldung kann bei Bedarf wieder aktiviert werden.

Informationen zu diesem Vorgang

Die erneute Aktivierung der Anmeldung über Fernzugriff für den `root`-Benutzer ist möglicherweise nicht erforderlich. Ein Benutzer mit den entsprechenden Berechtigungen kann die Befehle **`su`** und **`sudo`** verwenden, um als `root`-Benutzer zu arbeiten. Privilegierte Benutzer, die als `root` arbeiten, werden zu Prüfzwecken protokolliert.

IBM Intelligent Operations Center definiert den Benutzer `ibmadmin` in der Wheelgruppe. Benutzer in der Wheelgruppe können den Befehl **`sudo su -`** verwenden, um als `root` zu arbeiten.

Vorgehensweise

Gehen Sie wie folgt vor, um mithilfe des Befehls **`ssh`** die Rootanmeldung zu aktivieren.

1. Bearbeiten Sie die Datei `/etc/ssh/sshd_config` auf dem Server, auf dem Fernanmeldung als `root` über SSH oder ein fernes Terminal erforderlich ist.
2. Ändern Sie den Parameter `PermitRootLogin` auf `yes`, und speichern Sie die Datei. Ändern Sie diesen Parameter auf `no`, wenn die Anmeldung über Fernzugriff mithilfe des Befehls **`ssh`** inaktiviert sein muss.
3. Speichern Sie die Datei.

4. Starten Sie den SSH-Service neu, indem Sie den Befehl **service sshd restart** ausführen.

Cyber Hygiene inaktiviert die Anmeldung über Fernzugriff beim root-Konto mithilfe von fernen Terminals. Nur der Bildschirm und die Tastatur, die physisch mit dem Server verbunden sind, können sich als root-Benutzer anmelden. Gehen Sie wie folgt vor, um die root-Anmeldung über Fernzugriff an einen Server von einem fernen Terminal aus wieder zu aktivieren.

5. Bearbeiten Sie die Datei /etc/securetty auf dem Server, auf dem Fernanmeldung als root über SSH oder ein fernes Terminal erforderlich ist.
6. Fügen Sie die Linux-Einheitennamen für die Terminals hinzu, die für die ferne Anmeldung als root-Benutzer autorisiert sind. Wenn Sie z. B. tty1 hinzufügen möchten, ändern Sie die Liste folgendermaßen:

   ```
   console
   tty1
   ```

   Setzen Sie ein Rautezeichen (#) vor ein Terminal, das inaktiviert werden soll. Beispiel:

   ```
   console
   #tty1
   ```

7. Speichern Sie die Datei.

Benutzer für den SSH-Zugriff konfigurieren

Für IBM Intelligent Operations Center sind bestimmte Benutzer erforderlich, für die ein SSH-Zugriff und Kennwörter konfiguriert werden müssen.

Informationen zu diesem Vorgang

Die folgenden Benutzer müssen auf Installationsserver konfiguriert und alle Zielserver müssen für einen SSH-Zugriff und Kennwörter konfiguriert sein.

- ibmadmin
- ibmuser
- mqconn

Mit der Lösung bereitgestellte Tools installieren

Im Lieferumfang von IBM Intelligent Operations Center sind Toolkits und Entwicklungstools enthalten. Diese werden bei der Anpassung von IBM Intelligent Operations Center verwendet.

Mit Ausnahme von Rational Application Developer werden diese auf der Developer's Toolkit-DVD bzw. dem Image für IBM Intelligent Operations Center bereitgestellt. Rational Application Developer wird mit dem IBM Intelligent Operations Center auf separaten DVDs oder Images bereitgestellt.

Lotus Sametime Client

Informationen zum Installieren und Verwenden des Lotus Sametime Client finden Sie im Information Center für Lotus Domino und Lotus Notes.

WebSphere Message Broker-Toolkit

Informationen zum Installieren und Verwenden des WebSphere Message Broker-Toolkits finden Sie im Information Center für WebSphere Message Broker.

IBM WebSphere Business Monitor-Entwicklungstoolkit

Informationen zum Installieren und Verwenden des IBM WebSphere Business Monitor-Entwicklungstoolkits finden Sie im Information Center für IBM WebSphere Business Monitor.

Rational Application Developer

Informationen zum Installieren und Verwenden von Rational Application Developer finden Sie im Information Center für Rational Application Developer.

Zugehörige Konzepte:

„KPIs erstellen und integrieren" auf Seite 116
KPI-Modelle (Key Performance Indicator) können mit einem Entwicklungstoolkit zur Geschäftsüberwachung und einem KPI-Managementportlet erstellt und geändert werden.

Zugehörige Informationen:

Information Center für Lotus Domino und Lotus Notes

Information Center für WebSphere Message Broker

Information Center für IBM Business Monitor

Information Center für Rational Application Developer

Musterbenutzer löschen

Im Lieferumfang von IBM Intelligent Operations Center sind Musterbenutzer enthalten. Aus Sicherheitsgründen müssen diese Benutzer nach der Installation von IBM Intelligent Operations Center in einer Produktionsumgebung gelöscht werden.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um die vordefinierten Benutzer zu löschen:

Vorgehensweise

1. Melden Sie sich auf dem Anwendungsserver bei WebSphere Portal an.
2. Klicken Sie im Portal **Administration** auf **Zugriff** > **Benutzer und Gruppen** > **Alle authentifizierten Portalbenutzer**.
3. Klicken Sie für folgende Benutzer auf das Löschsymbol:
   - tdelorne
   - scollins
   - akelly

   Wichtig: Die folgenden Benutzer dürfen keinesfalls gelöscht werden, da sie erforderlich sind. Wenn Sie sie löschen, wird IBM Intelligent Operations Center nicht ordnungsgemäß ausgeführt.
   - admin
   - iicsystemuser
   - maxadmin
   - maxintadm
   - maxreg
   - notesadmin
   - resAdmin1
   - resDeployer1
   - resMonitor1
   - rtsAdmin
   - rtsConfig
   - rtsUser

- taiuser
- SRMSELFSERVICEUSR
- wasadmin
- waswebadmin
- wpsadmin
- wpsbind
- Alle Benutzer-IDs, die mit "PM" beginnen

Zugehörige Verweise:

„Musterbenutzer” auf Seite 75
Während der Implementierung des IBM Intelligent Operations Center werden Musterbenutzer erstellt.

Installationsservices aus dem Produktionssystem entfernen

Nach der Installation von IBM Intelligent Operations Center können die Installationsservices von den Produktionssystemservern entfernt werden. Es wird empfohlen, dass der Installationsserver beibehalten wird, da möglicherweise einige der Services für Verwaltungsaktivitäten benötigt werden.

Nach Abschluss und Prüfung der Installation können nur die Komponenten von den Produktionssystemservern (Anwendungsserver, Ereignisserver, Verwaltungsserver, Datenserver) entfernt werden, die im Installationsprozess verwendet wurden. Diese Komponenten sind:

- Das Verzeichnis, das von der Eigenschaft `Unix.image.basedir.remote` in der Eigenschaftendatei der Topologie definiert wurde.
- Das Verzeichnis, das von der Eigenschaft `Unix.script.basedir.remote` in der Eigenschaftendatei der Topologie definiert wurde.
- Das Verzeichnis *install_media*, das von der Eigenschaft `image.basedir.local` in der Eigenschaftendatei der Topologie definiert wurde.

Anmerkung: Der Installationsserver sollte für eine spätere Verwendung beibehalten werden. Da die Topologieeigenschaftendatei Kennwörter in Klartext enthält, sollte sich dieser Server an einem sicheren Ort befinden.

Zugehörige Tasks:

„IBM Intelligent Operations Center mithilfe des Installation Managers installieren” auf Seite 28
IBM Intelligent Operations Center kann mithilfe des bereitgestellten grafisch orientierten Installationsprogramms installiert werden.

Kapitel 3. Schutz der Lösung

Da das IBM Intelligent Operations Center bei entscheidenden Vorgängen eine zentrale Rolle einnimmt, ist die Sicherheit ein wichtiger Faktor. Zur Gewährleistung der Sicherheit ist es wichtig, dass Sie die Standardeinstellungen kennen. Auch die Verwaltung der Benutzer der Lösung ist unerlässlich, um allen Benutzern die jeweils richtige Zugriffsebene zuzuweisen.

Standardkennwörter

Zunächst müssen Sie zum Schutz der Lösung sicherstellen, dass alle Standardkennwörter geändert werden. Weitere Informationen zu den Standardkennwörtern erhalten Sie über den Link am Ende des Themas.

Sichere Verbindung

Für IBM Intelligent Operations Center ist HTTPS standardmäßig aktiviert. Sie können die HTTPS-Einstellungen für die folgenden einzelnen Services im IBM Intelligent Operations Center ändern:

- Den Geschäftsüberwachungsservice, mit dem KPIs verarbeitet werden
- Den Administrationsservice für Ressourcen und Standard Operating Procedures

Jede Änderung an den HTTPS-Einstellungen für einen einzelnen Service muss mit einer Aktualisierung der entsprechenden Porteinstellung einhergehen. Weitere Informationen zum Ändern dieser Einstellungen in der Tabelle mit Systemeigenschaften erhalten Sie über den Link am Ende des Themas.

Benutzerauthentifizierung

Die Benutzerauthentifizierung ist bestimmten Berechtigungen zugeordnet, die den Benutzerzugriff auf die entsprechenden Funktionen und Daten regeln. Das IBM Intelligent Operations Center unterstützt die Integration in die bereits vorhandene Sicherheitsinfrastruktur für die einmalige Anmeldung.

Die IBM Intelligent Operations Center-Benutzerberechtigungen werden durch WebSphere Portal-Benutzer und -Gruppen verwaltet. WebSphere Portal verwendet die Lightweight Directory Access Protocol-Datenbank (LDAP-Datenbank), die von dem Tivoli Directory Server bereitgestellt wird, der auf dem Datenserver ausgeführt wird.

Das vom IBM Intelligent Operations Center bereitgestellte Sicherheitssystem kann zahlreiche Benutzergruppen, Rollen und Berechtigungen beinhalten. Eine Vielzahl an Benutzergruppen, Rollen und Berechtigungen kann jedoch dazu führen, dass das Sicherheitssystem schwierig zu verwalten ist. Daher wird empfohlen, dass die Anzahl der Gruppen und Berechtigungen durch Administratoren beschränkt wird.

Benutzerrollen und Berechtigungen

Die Festlegung der Mitgliedschaft in einer rollenbasierten Benutzergruppe ermöglicht die Steuerung des Zugriffs auf das IBM Intelligent Operations Center. Die Benutzer in einer Gruppe können nur auf die Funktionen der Lösung zugreifen, die ihrer jeweiligen Rolle zugeordnet sind. Darüber hinaus können sich die Benutzer durch ihre Zugehörigkeit zu einer rollenbasierten Benutzergruppe gezielt auf Tasks konzentrieren, für die sie zuständig sind. Folgende Standardrollen stehen zur Verfügung: Entscheidungsträger, Aufsichtsperson und Betreiber.

So fügen Sie einen Benutzer dem IBM Intelligent Operations Center hinzu:

1. Wählen Sie eine Gruppe aus, die sich für die Rolle des Benutzers im Unternehmen eignet. Legen Sie den Benutzer dann als Mitglied der betreffenden Gruppe fest.

2. Erstellen Sie für den Benutzer ein Profil, das zumindest die Benutzer-ID, den Namen und das Kennwort enthält.

Datenkategorien und Berechtigungen

Die Sicherheit der Daten, die im IBM Intelligent Operations Center in Datenbanken gespeichert sind, wird durch die Implementierung eines rollenbasierten Zugriffs auf die Datenbanken verwaltet. Die Erteilung des Zugriffs auf eine Funktion des IBM Intelligent Operations Center bedeutet nicht, dass dem Benutzer sämtliche Daten zur Verfügung stehen. Die Steuerung der Datensicherheit erfolgt auf Serverebene, damit gewährleistet ist, dass Benutzer nur die gewünschten Daten anzeigen können. Die Standardkategorien lauten wie folgt: Geophysik, Verkehr, Wetter, Umwelt, Infrastruktur, Chemisch, Biologisch, Sicherheit, Recht und Ordnung, Rettungsdienst, Feuer, Gesundheit und Sonstige.

Portal

Der Portalservice stellt eine Plattform zur Verfügung, die für die erforderliche Benutzergruppe skaliert werden kann. Außerdem bietet sie einen rollenbasierten Zugriff, der an die erforderliche Organisationsstruktur angepasst werden kann. Mit dem Portlet **Manage Users and Groups** (Benutzer und Gruppen verwalten) können Sie Benutzer oder Benutzergruppen anzeigen, erstellen und löschen. Außerdem haben Sie die Möglichkeit, die Gruppenzugehörigkeiten zu ändern. Weitere Informationen zu diesem Portlet erhalten Sie über den Link am Ende dieses Themas.

Zugehörige Konzepte:

„Kennwortinformationen" auf Seite 41
Kennwörter für mehrere Benutzer-IDs, die in der IBM Intelligent Operations Center-Lösung verwendet werden, sind in der Datei mit den Topologieeigenschaften definiert. Aus Sicherheitsgründen sollten die mit IBM Intelligent Operations Center ausgelieferten Standardkennwörter geändert werden.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Benutzerrollen und Zugriff

Die Sicherheitsimplementierung im IBM Intelligent Operations Center erfolgt durch die benutzerrollenbasierte Einschränkung des Zugriffs auf Funktionen.

Um eine bestimmte Funktion des IBM Intelligent Operations Center verwenden zu können, muss ein Benutzer der Benutzerrollengruppe angehören, die den erforderlichen Zugriff auf die betreffende Funktion bereitstellt. Das Hinzufügen eines Benutzers zu einer Benutzerrollengruppe wird durch den Administrator vorgenommen. In der folgenden Tabelle ist beispielhaft dargestellt, wie die Zuordnung von realen Aufgabenbereichen zu den Benutzerrollengruppen mit Anmeldezugriffsebenen im IBM Intelligent Operations Center festgelegt sein könnte.

Tabelle 23. Aufgabenbereiche und Benutzerrollengruppen im IBM Intelligent Operations Center

Aufgabenbereich	Zuständigkeit	Benutzerrollengruppe
Entscheidungsträger	• Definiert Eingabeanforderungen und Schwellenwerte für Ereignisse, Vorfälle und Key Performance Indicators (KPIs) • Zeigt übergeordnete grafische Zusammenfassungen, Details und Berichte zu folgenden Punkten an: – KPIs – Ereignisse • Leitet Richtlinien, die langfristige Ausrichtung oder Entscheidungen auf Führungsebene weiter	Städtischer Entscheidungsträger

Tabelle 23. Aufgabenbereiche und Benutzerrollengruppen im IBM Intelligent Operations Center (Forts.)

Aufgabenbereich	Zuständigkeit	Benutzerrollengruppe
Aufsichtsperson oder Manager	• Verwaltet Ereignisse und Vorfälle • Erstellt und überwacht KPI-Berichte • Gibt Alerts aus • Analysiert Ereignisse im Hinblick auf Statusänderungen oder erforderliche Maßnahmen • Entscheidet über kurzfristige Korrekturmaßnahmen	Städtische Aufsichtsperson
Betreiber	• Überwacht Ereignisdaten • Überwacht Alerts • Zeigt Details an • Leitet Datenübertragungen ein • Aktualisiert Ereignis- oder Vorfallsdaten mit weiteren Informationen. Dazu zählen beispielsweise folgende Details: – Telefonische Berichte – Eingaben aus Baustellen oder Wartungsarbeiten	Städtischer Betreiber
Benutzeradministrator	Verwaltet sämtliche Benutzeraspekte. Dies umfasst die Definition von Gruppen, die Zuweisung von Berechtigungen zu Gruppen sowie die Zuweisung von Benutzern zu Gruppen. Stellt den Benutzern die richtige Zugriffsebene zur Verfügung. Die Zugriffsebene wird auf Grundlage der Gruppenzugehörigkeit zugewiesen.	wpsadmins

Machen Sie sich vor der Anpassung von Rollen und vor der Definition von Benutzern für Ihr Unternehmen mit dem Sicherheitssystem des IBM Intelligent Operations Center vertraut.

Zugehörige Tasks:

„Benutzer oder Gruppe hinzufügen" auf Seite 81
Wählen Sie eine Gruppe aus und erstellen Sie ein Benutzerprofil, um einen neuen Benutzer zum IBM Intelligent Operations Center hinzuzufügen. Wählen Sie einen Gruppennamen aus, um eine neue Gruppe hinzuzufügen.

Zugehörige Verweise:

„Benutzerrollengruppen und Berechtigungen" auf Seite 77
Jeder Benutzerrollengruppe ist ein Berechtigungssatz für den Zugriff auf die Funktionen im IBM Intelligent Operations Center zugeordnet.

„Benutzerkategoriegruppen und Datenberechtigungen" auf Seite 79
Die Berechtigung für den Zugriff auf eine Datenkategorie im IBM Intelligent Operations Center ist jeder einzelnen Benutzerkategoriegruppe zugeordnet.

Musterbenutzer

Während der Implementierung des IBM Intelligent Operations Center werden Musterbenutzer erstellt.

Generische Musterbenutzer sind mit Benutzerrollengruppen und den entsprechenden Zugriffsberechtigungen definiert. Diese Musterbenutzer sind lediglich als Beispiele definiert und werden in der folgenden Tabelle aufgelistet. Andere Benutzer sind für die Administration der Lösung erforderlich.

Tabelle 24. Im IBM Intelligent Operations Center definierte Benutzer

Benutzer-ID	**Benutzerrollengruppe**
Musterbenutzer	
tdelorne	Städtischer Entscheidungsträger
scollins	Städtische Aufsichtsperson
akelly	Städtischer Betreiber
Erforderlicher Benutzer	
wpsadmin	wpsadmins

Sobald Sie zum Definieren von Benutzern für Ihr Unternehmen bereit sind, löschen Sie nur die Musterbenutzer. Der Benutzer "wpsadmin" darf nicht gelöscht werden. Der Benutzer "wpsadmin" ist für Administrationstasks im Zusammenhang mit dem IBM Intelligent Operations Center wichtig. Weitere Informationen zu erforderlichen Benutzern erhalten Sie über den Link am Ende dieses Themas.

Wichtig: Ersetzen Sie das Standardkennwort des Benutzers "wpsadmin" durch ein neues Kennwort. Weitere Informationen zur Aktualisierung von Benutzer-IDs und Kennwörtern für Portaladministratoren finden Sie in der Dokumentation zu WebSphere Portal.

Zugehörige Konzepte:

„Kennwortinformationen" auf Seite 41
Kennwörter für mehrere Benutzer-IDs, die in der IBM Intelligent Operations Center-Lösung verwendet werden, sind in der Datei mit den Topologieeigenschaften definiert. Aus Sicherheitsgründen sollten die mit IBM Intelligent Operations Center ausgelieferten Standardkennwörter geändert werden.

Zugehörige Tasks:

„Musterbenutzer löschen" auf Seite 71
Im Lieferumfang von IBM Intelligent Operations Center sind Musterbenutzer enthalten. Aus Sicherheitsgründen müssen diese Benutzer nach der Installation von IBM Intelligent Operations Center in einer Produktionsumgebung gelöscht werden.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Benutzerrollengruppen und Berechtigungen

Jeder Benutzerrollengruppe ist ein Berechtigungssatz für den Zugriff auf die Funktionen im IBM Intelligent Operations Center zugeordnet.

Ein Administrator ordnet einem Benutzer eine Rolle zu, indem er den Benutzer als Mitglied der entsprechenden Benutzerrollengruppe festlegt. Jedem Benutzer ist die Mitgliedschaft in mindestens einer Benutzerrollengruppe zugeordnet.

In der folgenden Tabelle werden die Berechtigungen der einzelnen Benutzerrollengruppen aufgelistet, die mit dem IBM Intelligent Operations Center zur Verfügung gestellt werden. Jeder Benutzerrollengruppe wird für jede Funktion im IBM Intelligent Operations Center eine Berechtigung erteilt.

Tabelle 25. Funktionen im IBM Intelligent Operations Center und zugehörige Berechtigungen der Benutzerrollengruppen

Funktionstyp	**Funktionsname**	**Städtischer Entscheidungsträger**	**Städtische Aufsichtsperson**	**Städtischer Betreiber**	**wpsadmins**
Seite	Aufsichtsperson: Status	Benutzerberechtigung	Benutzerberechtigung	Keine	Administratorberechtigung
	Aufsichtsperson: Vorgänge	Benutzerberechtigung	Keine	Keine	Administratorberechtigung
	Aufsichtsperson: Berichte	Keine	Benutzerberechtigung	Keine	Administratorberechtigung
	Betreiber: Vorgänge	Keine	Keine	Benutzerberechtigung	Administratorberechtigung
	Betreiber: Berichte	Keine	Keine	Benutzerberechtigung	Administratorberechtigung
	Positionskarte	Keine	Benutzerberechtigung	Benutzerberechtigung	Administratorberechtigung
	Administration	Keine	Keine	Keine	Administratorberechtigung

Tabelle 25. Funktionen im IBM Intelligent Operations Center und zugehörige Berechtigungen der Benutzerrollengruppen (Forts.)

Portlet	Status	Benutzer-berechtigung	Benutzer-berechtigung	Keine	Administratorberechtigung
	Key Performance Indicator - Drilldown	Benutzer-berechtigung	Benutzer-berechtigung	Keine	Administratorberechtigung
	Benachrichtigun-gen	Benutzer-berechtigung	Benutzer-berechtigung	Benutzer-berechtigung	Administratorberechtigung
	Kontakt	Benutzer-berechtigung	Benutzer-berechtigung	Benutzer-berechtigung	Administratorberechtigung
	Karte	Benutzer-berechtigung	Keine	Benutzer-berechtigung	Administratorberechtigung
	Details	Benutzer-berechtigung	Keine	Benutzer-berechtigung	Administratorberechtigung
	Meine Aktivitä-ten	Benutzer-berechtigung	Benutzer-berechtigung	Benutzer-berechtigung	Administratorberechtigung
	Positionskarte	Keine	Benutzer-berechtigung	Benutzer-berechtigung	Administratorberechtigung
	Berichte	Keine	Benutzer-berechtigung	Benutzer-berechtigung	Administratorberechtigung
	Intelligent Ope-rations Center - Produktinforma-tionen	Keine	Keine	Keine	Administratorberechtigung
	Administrations-konsolen	Keine	Keine	Keine	Administratorberechtigung
	Systemprüfung	Keine	Keine	Keine	Administratorberechtigung
	Zusammen-fassung der Benutzerberech-tigungen	Keine	Keine	Keine	Administratorberechtigung
	Key Performance Indicators (KPIs)	Keine	Keine	Keine	Administratorberechtigung
	Positionskarten-manager	Keine	Keine	Keine	Administratorberechtigung
	Standard Opera-ting Procedures	Keine	Keine	Keine	Administratorberechtigung
	Erstellung von Ereignisscripts	Keine	Keine	Keine	Administratorberechtigung
	Beispiel-Publisher	Keine	Keine	Keine	Administratorberechtigung
	Benutzer und Gruppen	Keine	Keine	Keine	Administratorberechtigung

Die Zuordnung der IBM Intelligent Operations Center-Berechtigungen erfolgt auf Basis von Lightweight Directory Access Protocol-Gruppen (LDAP-Gruppen). Die Berechtigungen sind wie folgt definiert:

- Die "Benutzerberechtigung" ist die Berechtigung, die einem Benutzer erteilt wird, damit er Funktionen anzeigen und mit diesen arbeiten kann.

- Die "Administratorberechtigung" ist die Berechtigung, die einem Administrator erteilt wird, damit er mit seinem Zugriff folgende Aktionen ausführen kann:
  - Funktionen konfigurieren
  - Benutzer und Benutzergruppen erstellen, ändern oder löschen

Um auf die Daten des IBM Intelligent Operations Center zugreifen zu können, muss ein Benutzer der Benutzerkategoriegruppe angehören, die die erforderlichen Datenberechtigungen bereitstellt.

Zugehörige Konzepte:

„Zusammenfassung der Benutzerberechtigungen" auf Seite 86
Mit dem Portlet "Zusammenfassung der Benutzerberechtigungen" können Sie die den IBM Intelligent Operations Center-Benutzern und -Gruppen erteilten Berechtigungen anzeigen.

„Benutzerrollen und Zugriff" auf Seite 74
Die Sicherheitsimplementierung im IBM Intelligent Operations Center erfolgt durch die benutzerrollenbasierte Einschränkung des Zugriffs auf Funktionen.

Zugehörige Tasks:

„Benutzer oder Gruppe hinzufügen" auf Seite 81
Wählen Sie eine Gruppe aus und erstellen Sie ein Benutzerprofil, um einen neuen Benutzer zum IBM Intelligent Operations Center hinzuzufügen. Wählen Sie einen Gruppennamen aus, um eine neue Gruppe hinzuzufügen.

„Gruppenzugehörigkeit anzeigen oder ändern" auf Seite 82
Sie können die Gruppenzugehörigkeit anzeigen oder ändern, um die Zugriffsberechtigungen von Benutzern im IBM Intelligent Operations Center zu verwalten.

Zugehörige Verweise:

„Benutzerkategoriegruppen und Datenberechtigungen"
Die Berechtigung für den Zugriff auf eine Datenkategorie im IBM Intelligent Operations Center ist jeder einzelnen Benutzerkategoriegruppe zugeordnet.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Benutzerkategoriegruppen und Datenberechtigungen

Die Berechtigung für den Zugriff auf eine Datenkategorie im IBM Intelligent Operations Center ist jeder einzelnen Benutzerkategoriegruppe zugeordnet.

Ein Administrator ordnet einem Benutzer den Datenzugriff zu, indem er den Benutzer als Mitglied der entsprechenden Benutzerkategoriegruppe festlegt. Jedem Benutzer ist die Mitgliedschaft in mindestens einer Benutzerkategoriegruppe zugeordnet.

In der folgenden Tabelle werden die im IBM Intelligent Operations Center enthaltenen Datenkategorien sowie die entsprechenden Benutzerkategoriegruppen aufgelistet, über die Ereignisdaten, Key Performance Indicator-Daten (KPI-Daten) und Alertdaten bestimmt werden. Möchte ein Benutzer beispielsweise Ereignisse im Zusammenhang mit dem städtischen Wasserversorgungsamt anzeigen, muss er der Gruppe `ioc_base_infrastructure` angehören.

Tabelle 26. Beschreibungen und Kennungen der Benutzerkategoriegruppen

Datenkategorie	Beschreibung	Benutzerkategoriegruppe
CBRNE	Chemische, biologische, radiologische, nukleare und explosivstoffbezogene Bedrohungen und Angriffe	`ioc_base_chemical, ioc_base_biological, ioc_base_radiological, ioc_base_nuclear, ioc_base_explosive`
Umwelt	Umwelt: Umweltverschmutzung und sonstige Umweltereignisse	`ioc_base_environmental`

Tabelle 26. Beschreibungen und Kennungen der Benutzerkategoriegruppen (Forts.)

Daten-kategorie	Beschreibung	Benutzerkategoriegruppe
Feuer	Feuerbekämpfung und Rettungsdienst	`ioc_base_fire`
Geophysik	Geophysik (Naturkatastrophen wie Erdrutsche)	`ioc_base_geophysical`
Gesundheit	Medizinische Versorgung und Gesundheitsfürsorge	`ioc_base_health`
Infrastruktur	Infrastruktur: Versorgungsunternehmen, Telekommunikation, sonstige nicht verkehrsbezogene Infrastruktur	`ioc_base_infrastructure`
Wetter	Wetter (einschließlich Starkregen mit Hochwasser)	`ioc_base_meteorological`
Rettungsdienst	Rettung bei medizinischen Notfällen	`ioc_base_rescue`
Sicherheit	Allgemeine Notstände und öffentliche Sicherheit	`ioc_base_safety`
Recht und Ordnung	Strafverfolgung, Militär, Grenzschutz und Polizei	`ioc_base_security`
Verkehr	Öffentlicher und privater Verkehr	`ioc_base_transportation`
Sonstige	Sonstige Ereignisse, KPIs oder Alerts	`ioc_base_other`

Um sich anmelden und auf die Funktionen des IBM Intelligent Operations Center zugreifen zu können, muss ein Benutzer der Benutzerrollengruppe angehören, die die erforderlichen Berechtigungen bereitstellt.

Zugehörige Konzepte:

„Zusammenfassung der Benutzerberechtigungen" auf Seite 86
Mit dem Portlet "Zusammenfassung der Benutzerberechtigungen" können Sie die den IBM Intelligent Operations Center-Benutzern und -Gruppen erteilten Berechtigungen anzeigen.

„Benutzerrollen und Zugriff" auf Seite 74
Die Sicherheitsimplementierung im IBM Intelligent Operations Center erfolgt durch die benutzerrollenbasierte Einschränkung des Zugriffs auf Funktionen.

Zugehörige Tasks:

„Benutzer oder Gruppe hinzufügen" auf Seite 81
Wählen Sie eine Gruppe aus und erstellen Sie ein Benutzerprofil, um einen neuen Benutzer zum IBM Intelligent Operations Center hinzuzufügen. Wählen Sie einen Gruppennamen aus, um eine neue Gruppe hinzuzufügen.

„Gruppenzugehörigkeit anzeigen oder ändern" auf Seite 82
Sie können die Gruppenzugehörigkeit anzeigen oder ändern, um die Zugriffsberechtigungen von Benutzern im IBM Intelligent Operations Center zu verwalten.

Zugehörige Verweise:

„Benutzerrollengruppen und Berechtigungen" auf Seite 77
Jeder Benutzerrollengruppe ist ein Berechtigungssatz für den Zugriff auf die Funktionen im IBM Intelligent Operations Center zugeordnet.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Benutzer oder Gruppe hinzufügen

Wählen Sie eine Gruppe aus und erstellen Sie ein Benutzerprofil, um einen neuen Benutzer zum IBM Intelligent Operations Center hinzuzufügen. Wählen Sie einen Gruppennamen aus, um eine neue Gruppe hinzuzufügen.

Informationen zu diesem Vorgang

Wählen Sie zunächst eine Benutzerrollengruppe aus, damit beim Hinzufügen eines neuen Benutzers die richtige Ebene der Zugriffsberechtigungen festgelegt wird. Füllen Sie dann die Felder auf der Seite **Profile Management** (Profilverwaltung) aus, damit das IBM Intelligent Operations Center über die Informationen verfügt, die zum Hinzufügen des neuen Benutzers erforderlich sind. Folgen Sie dem Link am Ende des Themas, um weitere Informationen zu den Daten aufzurufen, die in den Feldern auf der Seite **Profile Management** (Profilverwaltung) eingegeben werden können.

Vorgehensweise

1. Melden Sie sich als Benutzer mit Verwaltungsaufgaben unter `http://app-host/wpsv70/wps/myportal/` an.
2. Klicken Sie in der Navigationsleiste oben auf der Seite auf **Administration**.
3. Klicken Sie in der Seitenleiste auf **Access** (Zugriff).
4. Klicken Sie im Untermenü auf **Users and Groups** (Benutzer und Gruppen).
5. Wenn Sie einen neuen Benutzer hinzufügen, wählen Sie eine Rolle aus, indem Sie den Benutzer als Mitglied einer Gruppe festlegen. Suchen Sie die Gruppe, indem Sie auf **All Portal User Groups** (Alle Portalbenutzergruppen) klicken, um eine Liste der Gruppen aufzurufen. Klicken Sie auf die erforderliche Gruppe.
6. Klicken Sie auf **New User** (Neuer Benutzer) oder **New Group** (Neue Gruppe).
7. Wenn Sie eine Benutzergruppe erstellen, geben Sie einen Namen für die Benutzergruppe ein.
8. Wenn Sie einen neuen Benutzer hinzufügen, stellen Sie sicher, dass Sie alle erforderlichen Felder im Benutzerprofil ausfüllen. Diese sind durch Sterne gekennzeichnet.
9. Klicken Sie auf **OK**, um das neue Profil oder die neue Gruppe zu übergeben.

Ergebnisse

In einer Nachricht wird der erfolgreiche Verlauf der Übergabe bestätigt. Ein neues Benutzerprofil wird erstellt und in der Gruppenliste angezeigt oder es wird eine neue Gruppe angezeigt. Der Zugriff des neuen Benutzers auf das IBM Intelligent Operations Center wird durch die Berechtigungen bestimmt, die der ausgewählten Rollengruppe zugeordnet sind.

Nächste Schritte

- Weisen Sie dem neuen Benutzer unter Berücksichtigung der erforderlichen Datenberechtigungen die hierfür geeignete Mitgliedschaft in den Datenkategoriegruppen zu.
- Wenn eine neue Gruppe hinzugefügt wurde, muss sie auch in die WebSphere Application Server Network Deployment-Junction-ACL aufgenommen werden.
- Sie müssen außerdem Berechtigungen für eine neu hinzugefügte Gruppe festlegen. Über die Berechtigungen wird definiert, welche Funktionen und Daten von den Gruppenmitgliedern angezeigt und geändert werden können. Informationen zum Festlegen von Berechtigungen finden Sie über den Link zur Produktdokumentation zu IBM WebSphere Portal 7 am Ende des Themas und suchen Sie nach den Informationen zum Zuweisen von Zugriff auf Seiten.
- Ordnen Sie den neuen Benutzer einer Sicherheitsgruppe und Personengruppe in Tivoli Service Request Manager zu.

Anmerkung: Um Zeit zu sparen, können Sie die Gruppenzuordnungen eines bereits vorhandenen Benutzers für einen neuen Benutzer duplizieren. Wählen Sie den neuen Benutzer aus und klicken Sie auf das Symbol **Duplicate** (Duplizieren). Wählen Sie den bereits vorhandenen Benutzer aus, um die Gruppenzugehörigkeit zu duplizieren.

Zugehörige Konzepte:

„Benutzerrollen und Zugriff" auf Seite 74
Die Sicherheitsimplementierung im IBM Intelligent Operations Center erfolgt durch die benutzerrollenbasierte Einschränkung des Zugriffs auf Funktionen.

Zugehörige Tasks:

„Neue Benutzer in Tivoli Service Request Manager konfigurieren" auf Seite 133
Wenn Sie einen Benutzer in IBM Intelligent Operations Center hinzufügen, ordnen Sie Berechtigungen und Personengruppen für den Benutzer in Tivoli Service Request Manager zu.

Zugehörige Verweise:

„Benutzerrollengruppen und Berechtigungen" auf Seite 77
Jeder Benutzerrollengruppe ist ein Berechtigungssatz für den Zugriff auf die Funktionen im IBM Intelligent Operations Center zugeordnet.

„Benutzerkategoriegruppen und Datenberechtigungen" auf Seite 79
Die Berechtigung für den Zugriff auf eine Datenkategorie im IBM Intelligent Operations Center ist jeder einzelnen Benutzerkategoriegruppe zugeordnet.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Gruppenzugehörigkeit anzeigen oder ändern

Sie können die Gruppenzugehörigkeit anzeigen oder ändern, um die Zugriffsberechtigungen von Benutzern im IBM Intelligent Operations Center zu verwalten.

Informationen zu diesem Vorgang

Wählen Sie die Gruppe aus, die der Rolle oder Datenkategorie entspricht, für die Sie die Mitgliedschaft anzeigen oder ändern möchten. Durch die Zugehörigkeit zu einer Rollengruppe erhalten die Benutzer Zugriff auf die Bereiche der Lösung, die der jeweiligen Rolle zugeordnet sind. Die Zugehörigkeit zu einer Kategoriegruppe ermöglicht den Benutzern den Zugriff auf die Ereignisse, Key Performance Indicators (KPIs) und Alerts, die der betreffenden Kategorie zugeordnet sind.

Bewegen Sie die Maus über ein Symbol, um die zugehörige Direkthilfe aufzurufen, in der der Zweck des Symbols angegeben wird.

Vorgehensweise

1. Melden Sie sich als Benutzer mit Verwaltungsaufgaben unter `http://app-host/wpsv70/wps/myportal/` an.
2. Klicken Sie in der Navigationsleiste oben auf der Seite auf **Administration**.
3. Klicken Sie in der Seitenleiste auf **Access** (Zugriff).
4. Klicken Sie im Untermenü auf **Users and Groups** (Benutzer und Gruppen).
5. Klicken Sie auf **All Portal User Groups** (Alle Portalbenutzergruppen), um eine Liste der Gruppen aufzurufen. Klicken Sie auf die erforderliche Gruppe. Die Mitglieder der Gruppe werden aufgelistet.
6. Im Zusammenhang mit der Gruppenzugehörigkeit können die folgenden Aktionen ausgeführt werden:
   - Zeigen Sie die Zugehörigkeit zu anderen Gruppen an, indem Sie für die Benutzer-ID auf **View membership** (Zugehörigkeit anzeigen) klicken.

- Fügen Sie der Gruppe einen oder mehrere Benutzer hinzu, indem Sie auf **Add member** (Mitglied hinzufügen) klicken und den bzw. die hinzuzufügenden Benutzer auswählen.
- Entfernen Sie einen Benutzer aus der Gruppe, indem Sie für die Benutzer-ID auf **Remove** (Entfernen) klicken.

Zugehörige Verweise:

„Benutzerrollengruppen und Berechtigungen" auf Seite 77
Jeder Benutzerrollengruppe ist ein Berechtigungssatz für den Zugriff auf die Funktionen im IBM Intelligent Operations Center zugeordnet.

„Benutzerkategoriegruppen und Datenberechtigungen" auf Seite 79
Die Berechtigung für den Zugriff auf eine Datenkategorie im IBM Intelligent Operations Center ist jeder einzelnen Benutzerkategoriegruppe zugeordnet.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Benutzerprofil anzeigen oder bearbeiten

Zeigen Sie das Profil eines Benutzers an oder bearbeiten Sie es, um die Benutzerprofilattribute festzulegen oder zurückzusetzen. Dies gilt auch für das Kennwort. Die Benutzer-ID kann nicht geändert werden.

Informationen zu diesem Vorgang

Wählen Sie den Benutzer aus der Liste der authentifizierten Portalbenutzer aus, um das Benutzerprofil zu öffnen und die Profilzusatzinformationen zu ändern. Außerdem kann jeder Benutzer sein eigenes Profil ändern.

Bewegen Sie die Maus über ein Symbol, um die zugehörige Direkthilfe aufzurufen, in der der Zweck des Symbols angegeben wird.

Vorgehensweise

1. Melden Sie sich als Benutzer mit Verwaltungsaufgaben unter `http://app-host/wpsv70/wps/myportal/` an.
2. Klicken Sie in der Navigationsleiste ganz oben auf **Administration**.
3. Klicken Sie im Seitenleistenmenü auf **Access** (Zugriff).
4. Klicken Sie im Untermenü auf **Users and Groups** (Benutzer und Gruppen).
5. Klicken Sie auf **All Authenticated Portal Users** (Alle authentifizierten Portalbenutzer), um eine Liste der Benutzer aufzurufen.
6. Klicken Sie auf das Bearbeitungssymbol für den Benutzer, um die Seite **Profile Management** (Profilverwaltung) anzuzeigen. Die Attributfelder für das Benutzerprofil werden angezeigt.
7. Wenn Sie das Kennwort ändern möchten, geben Sie in den Feldern **New Password:** (Neues Kennwort:) und **Confirm Password:** (Kennwort bestätigen:) ein neues Kennwort ein.
8. Sie können in den übrigen Feldern beliebig Informationen eingeben, bearbeiten oder löschen.
9. Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu übergeben.

Ergebnisse

Das Benutzerprofil wird mit den von Ihnen übergebenen Änderungen aktualisiert.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Benutzer oder Gruppe löschen

Sie können einen Benutzer oder eine Gruppe aus dem IBM Intelligent Operations Center löschen.

Informationen zu diesem Vorgang

Wenn Sie einen Benutzer löschen möchten, wählen Sie diesen aus der Liste der authentifizierten Portalbenutzer aus und löschen Sie ihn. Wenn Sie eine Gruppe löschen möchten, wählen Sie die Gruppe aus der Liste der Portalbenutzergruppen aus und löschen Sie sie.

Bewegen Sie die Maus über ein Symbol, um die zugehörige Direkthilfe aufzurufen, in der der Zweck des Symbols angegeben wird.

Anmerkung: Beachten Sie, dass durch das Löschen eines Benutzers im IBM Intelligent Operations Center auch dessen Zugriff auf andere Lösungen in der Produktfamilie IBM Smarter Cities™ Software Solutions entfernt wird. Wird eine Gruppe gelöscht, wird sie auch aus anderen Lösungen entfernt.

Vorgehensweise

1. Melden Sie sich als Benutzer mit Verwaltungsaufgaben unter `http://app-host/wpsv70/wps/myportal/` an.
2. Klicken Sie in der Navigationsleiste ganz oben auf **Administration**.
3. Klicken Sie in der Seitenleiste auf **Access** (Zugriff).
4. Klicken Sie im Untermenü auf **Users and Groups** (Benutzer und Gruppen):
   - Klicken Sie auf **All Portal User Groups** (Alle Portalbenutzergruppen), um eine Liste der Gruppen aufzurufen.
   - Klicken Sie auf **All Authenticated Portal Users** (Alle authentifizierten Portalbenutzer), um eine Liste der Benutzer aufzurufen.
5. Klicken Sie auf das Symbol **Delete** (Löschen), das dem Benutzer oder der Gruppe zugeordnet ist, den bzw. die Sie löschen möchten.

Ergebnisse

Sobald Sie einen Benutzer oder eine Gruppe gelöscht haben, ist dieser bzw. diese nicht mehr im IBM Intelligent Operations Center vorhanden. Die Mitglieder der Gruppe werden durch das Löschen einer Gruppe nicht gelöscht.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Benutzer und Gruppen importieren

Über den Portalservice können Sie Benutzer in Gruppen in IBM Intelligent Operations Center importieren.

Informationen zu diesem Vorgang

Über die Portaladministrationskonsole können Sie als Portaladministrator Benutzer in Gruppen in IBM Intelligent Operations Center importieren. Die für diese Task erforderliche XML-Datei befindet sich auf dem Anwendungsserver unter: `/opt/IBM/WebSphere/PortalServer/doc/xml-samples/CreateUser.xml`. Diese XML-Datei kann geändert werden, um Benutzer zum IBM Intelligent Operations Center hinzuzufügen.

Anmerkung: Wenn Sie mehrere Benutzer hinzufügen, fügen Sie zuerst alle Benutzer hinzu, bevor Sie die Benutzer zu Gruppen hinzufügen. Ein Beispiel hierfür finden Sie am Ende des Themas.

Alternativ zur folgenden Vorgehensweise können Sie den Befehl über die Befehlszeile des Scripts `xmlaccess.sh` ausführen, das sich auf dem Anwendungsserver befindet.

Vorgehensweise

1. Aktualisieren Sie die Datei `CreateUser.xml` so, dass sie neue Benutzer und die dazugehörigen Gruppen enthält.
2. Melden Sie sich als Benutzer mit Verwaltungsaufgaben unter http://*app-host*/wpsv70/wps/myportal/an.
3. Klicken Sie auf **Administration**.
4. Klicken Sie unter **Portaleinstellungen** auf **XML importieren**.
5. Suchen Sie nach der aktualisierten XML-Datei.
6. Klicken Sie auf **Importieren**.

Ergebnisse

Der WebSphere Portal Server erstellt automatisch die zugehörigen Einträge im Verzeichnis auf dem Tivoli Directory Server und in Tivoli Access Manager WebSEAL.

Beispiel

Im folgenden Beispiel wird die XML-Datei so geändert, dass zwei Benutzer zum IBM Intelligent Operations Center und jeder Benutzer zu einer Rollengruppe und einer Kategoriegruppe hinzugefügt werden.

```
<?xml version="1.0" encoding="UTF-8"?>
<request xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PortalConfig_7.0.0.xsd" type="update"
create-oids="true">
<portal action="locate">
<user action="update" name="cityuser003" firstname="City"
lastname="user003" password="passw0rd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user003</parameter>
</user>
<user action="update" name="cityuser004" firstname="City"
lastname="user003" password="passw0rd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user004</parameter>
</user>
<group action="update" name="City Executive">
<member-user update="set" id="cityuser003">
</group>
<group action="update" name="ioc_base_fire">
<member-user update="set" id="cityuser003">
<group action="update" name="City Executive">
<member-user update="set" id="cityuser004">
</group>
<group action="update" name="ioc_base_fire">
<member-user update="set" id="cityuser004">
</group>
</portal>
</request>
```

Zugehörige Konzepte:

„Administrationskonsolen” auf Seite 213
Mit dem Portlet "Administrationskonsolen" können Sie die Services verwalten, die von der Lösung bereitgestellt werden.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Tivoli Directory Server Information Center

Tivoli Access Manager Information Center

Zusammenfassung der Benutzerberechtigungen

Mit dem Portlet "Zusammenfassung der Benutzerberechtigungen" können Sie die den IBM Intelligent Operations Center-Benutzern und -Gruppen erteilten Berechtigungen anzeigen.

Im Portlet "Zusammenfassung der Benutzerberechtigungen" werden Details zur Gruppenzugehörigkeit und zu den erteilten Benutzerberechtigungen angezeigt.

Um auf das Portlet "Zusammenfassung der Benutzerberechtigungen" zuzugreifen, klicken Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Administration Tools** > **User Permissions Summary** (Intelligent Operations > Verwaltungstools > Zusammenfassung der Benutzerberechtigungen).

Auf der Registerkarte für Benutzer können Sie die einem Benutzer erteilten Berechtigungen überprüfen. Bei Eingabe der Benutzer-ID werden folgende Informationen angezeigt:

- Eine vollständige Liste aller in IBM Intelligent Operations Center verfügbaren Datenkategorien und Benutzerkategoriegruppen.
- Eine Liste der dem Benutzer zugeordneten Datenkategorieberechtigungen.
- Eine Liste aller Gruppen, Benutzerrollengruppen und Benutzerkategoriegruppen, zu denen der Benutzer gehört.
- Eine Liste der einzelnen Datenkategorien; zu jeder Datenkategorie ist angegeben, ob der Benutzer über eine Berechtigung für diese Kategorie verfügt.

Auf der Registerkarte **Zusammenfassung** können Sie die Übersichtsstatik für Benutzer und Gruppenberechtigungen anzeigen. Folgende Informationen werden angezeigt:

- Die Gesamtanzahl der Gruppen in IBM Intelligent Operations Center.
- Die Gesamtanzahl der Benutzer, denen eine Zugriffsberechtigung für IBM Intelligent Operations Center erteilt wurde.
- Eine Liste mit allen Benutzern nach Datenkategorie.
- Eine Liste mit allen Benutzern nach Benutzerrollengruppe.

Zugehörige Verweise:

„Benutzerrollengruppen und Berechtigungen" auf Seite 77
Jeder Benutzerrollengruppe ist ein Berechtigungssatz für den Zugriff auf die Funktionen im IBM Intelligent Operations Center zugeordnet.

„Benutzerkategoriegruppen und Datenberechtigungen" auf Seite 79
Die Berechtigung für den Zugriff auf eine Datenkategorie im IBM Intelligent Operations Center ist jeder einzelnen Benutzerkategoriegruppe zugeordnet.

Übersicht über Cyber Hygiene

Das IBM Intelligent Operations Center-Feature Cyber Hygiene stellt Services bereit, um gegen potenzielle Sicherheitsrisiken im installierten System vorzugehen.

Anmerkung: Allgemein werden mit dem Begriff 'Schwachstelle" sowohl Sicherheitsschwachstellen als auch Sicherheitsrisiken bezeichnet. Cyber Hygiene definiert eine Schwachstelle als einen Programmierfehler in einer Anwendung, der Sicherheitsverletzungen zur Folge haben kann. Als "Sicherheitsrisiko" bezeichnet Cyber Hygiene ein Betriebssystem oder eine Anwendungskonfiguration, die wenig Sicherheit bietet. Sicherheitsrisiken können durch die Auswahl einer sichereren Konfigurationsoption beseitigt werden. Ein Verzeichnis kann zum Beispiel so konfiguriert werden, dass sämtliche Benutzer dort Dateien speichern können. Es kann aber auch eine sicherere Konfiguration gewählt werden, sodass lediglich der Eigner die Berechtigung besitzt, Dateien in dem Verzeichnis zu speichern.

Cyber Hygiene umfasst zwei wesentliche Aspekte:

- Entschärfung und Korrektur von bekannten Sicherheitsrisiken im Betriebssystem Linux und den zugehörigen Benutzern, Verzeichnissen und Dateien. Dies geschieht durch eine Reihe von Tools und Scripts.
- Dokumentation der Prüfung von fast 1000 bekannten Schwachstellen und Sicherheitsrisiken beim Betriebssystem, bei den Produkten und bei der Systemkonfiguration.

Durch die Behandlung von Sicherheitsrisiken während des Installationsprozesses ist es für den Kunden weniger aufwendig, eine höhere Sicherheitsstufe im implementierten System zu erreichen.

Eine Regierungsbehörde kann z. B. die Funktionen für Problemlösung und Dokumentation von Cyber Hygiene nutzen, um Zertifizierung und Akkreditierung des Systems für die Implementierung in einem sicheren Netz zu unterstützen. Gewerbliche Geschäftskunden können denselben Prozess verwenden, um die Sicherheit ihrer Umgebung zu verbessern.

Cyber Hygiene bietet Risikominderung, nicht aber Risikoprävention. Da Systeme ausgeführt werden und zugänglich sein müssen, um von Wert zu sein, besteht immer das Risiko, dass die Informationen oder die Steuerung eines Systems beeinträchtigt werden.

Cyber Hygiene geht nicht gegen anwendungsspezifische Schwachstellen vor, die einschließen, wie Bedrohungen wie Denial of Service, SQL-Injection usw. von der Anwendung behandelt werden. Stattdessen bietet Cyber Hygiene eine Basis für die Anwendungssicherheit, indem es allgemein gegen Sicherheitsrisiken bei den Benutzern, Verzeichnissen und Dateien vorgeht und dieses Vorgehen nicht auf eine bestimmte Anwendung beschränkt. Cyber Hygiene wird nach der Produktinstallation ausgeführt, um diese allgemeinen Schwachstellen des Systems sowie von Anwendungsbenutzern, Verzeichnissen und Dateien zu korrigieren. Jede mit dem Betriebssystem Linux verwendete Anwendung muss getrennt in Bezug auf anwendungsspezifische Schwachstellen bewertet werden.

Der Katalog der bekannten Schwachstellen und Sicherheitsrisiken, der in Cyber Hygiene verwendet wird, basiert auf nicht klassifizierten, nicht vertraulichen Prüflisten der Defense Information Services Agency (DISA) der Vereinigten Staaten. Die Elemente auf diesen Listen werden auf ihre Anwendbarkeit auf Cyber Hygiene geprüft. Scan-Scripts suchen nach Instanzen eines Sicherheitsrisikos und protokollieren sie. Dann werden, soweit zutreffend, die Protokolldateien als Eingabe für Korrekturscripts gegen dieses Problem verwendet. Ein kleines Subset von Sicherheitsergebnissen benötigt eine andere Bearbeitung.

Die Dokumentation, die bekannte Schwachstellen in Komponenten von IBM Intelligent Operations Center und die von Cyber Hygiene durchgeführten Maßnahmen zu ihrer Minderung auflistet, wird durch IBM Intelligent Operations Center bereitgestellt.

Zugehörige Tasks:

„Prüfliste - Installation mithilfe des IBM Installation Manager" auf Seite 16
Verwenden Sie diese Prüfliste, um die Installationsschritte nachzuverfolgen, wenn Sie IBM Intelligent Operations Center mithilfe vonIBM Installation Manager installieren.

„Prüfliste - Schrittweise Installation" auf Seite 18
Verwenden Sie diese Prüfliste, um die Installationsschritte nachzuverfolgen, wenn Sie IBM Intelligent Operations Center mithilfe von Scripts und Befehlen installieren.

„IBM Intelligent Operations Center mithilfe des Installation Managers installieren" auf Seite 28
IBM Intelligent Operations Center kann mithilfe des bereitgestellten grafisch orientierten Installationsprogramms installiert werden.

„Cyber Hygiene schrittweise installieren und ausführen" auf Seite 66
Cyber Hygiene wird getrennt von IBM Intelligent Operations Center installiert und ausgeführt und zwar erst, nachdem alle anderen Komponenten von IBM Intelligent Operations Center installiert, konfiguriert und aktiv sind. Cyber Hygiene ersetzt die Standardbetriebssystemkonfiguration durch eine Reihe sicherere Optionen, die die Sicherheitsbasis des IBM Intelligent Operations Center-Systems grundlegend verbessern.

Cyber-Sicherheit

Die Sicherheit der IT-Umgebung ist seit langem ein Anliegen nationaler Regierungen und wird für kritische Infrastruktursysteme immer wichtiger. Bei Produkten und Lösungen mit kritischer Infrastruktur, z. B. IBM Intelligent Operations Center, sollten nach Möglichkeit bekannte Schwachstellen behoben werden, bevor diese Produkte und Lösungen verfügbar gemacht werden.

Cyber-Sicherheit bietet eine Risikominderung, aber keine Risikoprävention. Da IT-Systeme ausgeführt werden müssen und zugänglich sein sollten, um von Wert zu sein, besteht immer das Risiko, dass die Informationen oder die Steuerung eines Systems beeinträchtigt werden. Cyber-Sicherheit besteht sowohl aus statischen als auch dynamischen Elementen. Cyber Hygiene in IBM Intelligent Operations Center spricht die statischen Elemente der Cyber-Sicherheit an. Um die dynamischen Elemente der Cyber-Sicherheit anzusprechen, werden andere Tools und Prozesse benötigt. Diese Tools und Prozesse können physische und Personal-Sicherheitsprozeduren oder Tools gegen ein Eindringen in das Netzwerk von außen enthalten.

Die Cyber Hygiene-Funktionen von IBM Intelligent Operations Center sind für Bereiche wie schwache Sicherheitskonfigurationen, Softwarefehler, Systemverwaltungsfehler und Prozessfehler bei der Systemsicherheit ausgelegt. Um diesen Support bereitzustellen, bietet Cyber Hygiene Installations- und Konfigurationsfunktionen, die das Betriebssystem und die Verwaltungsfunktionen konfigurieren, damit sichere Einstellungen festgelegt und wichtige sicherheitsrelevante Fix-Packs installiert werden. Systeme werden zum Beispiel so konfiguriert, dass es keine Benutzer-ID ohne Kennwort gibt und dass unsichere Linux-Services wie FTP, SNMP und RLOGIN inaktiviert sind. Systeme können jedoch zur Erfüllung von spezifischen Sicherheitsverfahren von Unternehmen nicht automatisch konfiguriert werden.

Cyber Hygiene-Checklisten

Cyber Hygiene verwendet Checklisten, die auf den DISA-Checklisten (Defense Information Systems Agency) und periodischen Alerts für Schwachstellen basieren.

Analyse der Prüflistenelemente

Jede in der uneingeschränkten DISA-Checkliste (Defense Information System Agency) festgestellte Schwachstelle definiert Daten in Bezug auf diese Schwachstelle.

Die Informationen zu jeder Schwachstelle sind unter anderem folgende:

- Eine eindeutige ID. Die ID besteht aus einer STIG-ID (Security Implementation Technical Guide) und einem VMS-Schlüssel (Vulnerability Management System).

- Ein kurzer Name, der die Schwachstelle zusammenfasst.
- Der Schweregrad der Schwachstelle. Die dokumentierten Schweregrade lauten wie folgt:

  I Hoher Schweregrad

  II Mittlerer Schweregrad

  III Geringer Schweregrad
- Das betroffene Produkt bzw. die betroffenen Produkte.
- Die betroffene Produktversion bzw. die betroffenen Produktversionen.
- Eine Beschreibung der Schwachstelle, einschließlich Anwendungsfälle, Kontext oder Interaktionen mit anderer Software.
- Alle empfohlenen Aktionen. Wenn eine Korrektur über Patches oder Aktualisierungen nicht möglich ist, ist eine empfohlene Risikominderung enthalten.
- Alle Alerts, die den Alert außer Kraft setzen.

Bei jeder Schwachstelle muss festgestellt werden, ob sie sich negativ auf IBM Intelligent Operations Center auswirkt. Beispiel:

- Ist das Produktrelease und der Fix-Level im Lieferumfang von IBM Intelligent Operations Center betroffen? Ein früheres Produktrelease oder ein früherer Fix-Level sind eventuell nicht betroffen, da das Problem erst bei einem höheren Release oder Fix auftreten kann.
- Wird das Produkt im Lieferumfang von IBM Intelligent Operations Center so verwendet, dass eine Schwachstelle auftreten könnte? Ein Problem kann beispielsweise nur auftreten, wenn das Produkt Services eines anderen Produkts verwendet. Wenn diese Services in der IBM Intelligent Operations Center-Konfiguration nicht verwendet werden, ist eine Korrektur gegebenenfalls nicht erforderlich.
- Wirkt sich die Produktanfälligkeit auf das verwendete Betriebssystem aus? Einige Schwachstellen können nur auftreten, wenn bestimmte Betriebssysteme ausgeführt werden.

Diese Faktoren werden für jedes Element in der Checkliste analysiert, um die Aktion zu bestimmen, die für IBM Intelligent Operations Center notwendig ist. Diese Analyse und Korrektur führt zu einer der folgenden vier Bewertungen:

Not Applicable (NA) - Nicht zutreffend (NA)
Das betroffene Produkt bzw. die betroffene Konfiguration ist kein Teil der IBM Intelligent Operations Center-Umgebung.

Not a Finding (NF) - Kein Ergebnis (NF)
Die installierte Version oder der installierte Fix-Level des Produkts ist nicht betroffen oder das Produkt wird so verwendet, dass keine Schwachstelle auftreten kann. Diese Bewertung wird auch verwendet, wenn die Konfiguration die Schwachstelle nicht offenlegt.

Open - Offen
Die Schwachstelle bezieht sich auf die installierte Produktversion und auf den installierten Fix-Level. Es ist jedoch keine Korrektur für das Produkt verfügbar. Diese Bewertung wird auch verwendet, wenn das System so konfiguriert ist, dass die Schwachstelle offengelegt wird. Beispiel: Das Zulassen von globalen Schreibberechtigungen für ein Verzeichnis, das das Produkt benötigt. Diese Bewertung wird außerdem verwendet, wenn das Anwenden einer Korrektur von Organisationsrichtlinien, z. B. Kennwortrichtlinien zur Länge oder zu Zeichen, abhängig ist.

Fixed - Gelöst
Eine Korrektur einer offenen Schwachstelle wurde angewendet und überprüft.

In Tabelle 27 auf Seite 90 wird ein Beispiel einer Analyse dargestellt. Im zweiten Beispiel wird die Handhabung eines Produkts gezeigt, das auf keinem IBM Intelligent Operations Center-Server installiert ist.

Tabelle 27. Beispiel von Schwachstellenbewertungen

ID	Name	Schwere-grad	Anwendungs-server	Ereignis-server	Datenserver	Verwaltungsserver	Erläuterung
2011-B-0082	Mehrere Schwachstellen in IBM Websphere Application Server	I	NF	Open (Offen)	NA	NF	Betrifft Versionen vor 6.1.0.39 und 7.0.0.19
2011-B-0085	Mehrere DoS-Schwachstellen in Wireshark	I	NA	NA	NA	NA	Wireshark nicht installiert

Auswahl von Checklisten

Die Checklisten, die für jeden Server verwendet werden, basieren auf der Software, die auf dem jeweiligen Server installiert ist. Spezifische Checklisten sprechen Schwachstellen für Produkttypen an, z. B. Datenbanken. Andere Checklisten hingegen sind für Probleme mit bestimmten Produkten innerhalb einer Kategorie ausgelegt, z. B. DB2.

Nicht alle Produkttypen haben spezifische Checklisten. Allgemeine Schwachstellen werden in der Checkliste für die Anwendungssicherheit oder in einer betriebsystemrelevanten Liste dokumentiert.

Folgende Typen von Checklisten werden von Cyber Hygiene verwendet:

Application security (Anwendungssicherheit)
: Listet Schwachstellen auf Systemebene auf. Einige Checklisten beziehen sich auf die Softwareentwicklung und Testverfahren und andere beziehen sich auf anwendungsspezifische Schwachstellen, z. B. nicht verwendete verschlüsselte Kennwörter während der Benutzerauthentifizierung.

Unix/Linux
: Listet Schwachstellen in Bezug auf Konfiguration, Kennwortverwaltung, Dateisystempartionierung usw. auf.

Web Server (Web-Server)
: Listet Schwachstellen in Bezug auf HTTP-Server auf.

Database (Datenbank)
: Listet Schwachstellen in Bezug auf Datenbankserver auf.

Directory Servers (Verzeichnisserver)
: Listet Schwachstellen in Bezug auf LDAP-Server auf.

Enterprise System Management
: Listet Schwachstellen in Bezug auf Tools für die Unternehmenssystemverwaltung und für Systemverwaltungsprozesse auf.

Die Netzwerksicherheit wird von den Checklisten nicht abgedeckt, da die Konfiguration der Netzwerksicherheit von den Richtlinien und der Netzwerkarchitektur des Kunden bestimmt wird. Die Konfiguration der Netzwerksicherheit wird je nach den Anforderungen jeder Installation durchgeführt.

Standardkonfiguration von Cyber Hygiene

Mit der Cyber Hygiene-Funktion werden Linux-Standardkonfigurationen und Richtlinien auf sicherere Optionen festgelegt als in der Standard-Betriebssysteminstallation. Diese Standardeinstellungen lassen sich von Systemadministratoren ohne großen Aufwand so ändern, dass sie den Sicherheitsrichtlinien für die Installation entsprechen.

Die Administrationsgruppe für den IT-Betrieb eines Unternehmens ist für die Sicherheit ihrer System verantwortlich. Dazu gehören die Verwaltung des Netzwerkzugriffs sowie interne Sicherheitsrichtlinien und -prozesse.

Wenn Cyber Hygiene-Standardeinstellungen nicht den Unternehmensrichtlinien entsprechen, haben Unternehmensrichtlinien Vorrang. Denken Sie daran, dass nicht getestet wurde, wie sich lokale Einstellungen der Sicherheitsrichtlinien auf die Systemfunktionalität auswirken. Gehen Sie beim Anwenden von Sicherheitsrichtlinien auf Produkte, die nicht mit Cyber Hygiene implementiert wurden, mit derselben Vorsicht vor wie beim Anwenden der Sicherheitsrichtlinie auf IBM Intelligent Operations Center.

Weil IBM Intelligent Operations Center für einzelne Sicherheitsrichtlinien des Unternehmens nicht automatisch konfiguriert werden kann, kann IBM Intelligent Operations Center so konfiguriert werden, dass bekannte Schwachstellen entfernt werden. Cyber Hygiene konfiguriert IBM Intelligent Operations Center mit einem Satz an standardisierten Best-Practices-Richtlinien, die eine Grundlage für Systemadministratoren sind, die zum Anwendung bestimmter Unternehmensrichtlinien und -Verfahren verwendet werden können.

Managementrichtlinien zum Standardkennwort

Cyber Hygiene konfiguriert die standardmäßigen Kennwortmanagementrichtlinien des Betriebssystems Linux.

Die von Cyber Hygiene festgelegten standardmäßigen Managementrichtlinien für Kennwörter sind in Tabelle 28 angegeben.

Tabelle 28. Standardmäßige Kennwortmanagementrichtlinien bei Cyber Hygiene

Richtlinie	**Wert oder Einstellung**
Minimale Kennwortlänge	8 Zeichen
Zulässige Zeichen	Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen (: ; ! ` ~ @ # $ % ^ & * ( ) - _ = + [{] } \ | ' " , < . > / ? und das Leerzeichen)
Inhaltliche Vorgaben	keine
Zulässige Zahl an fehlgeschlagenen Anmeldeversuchen für einen Benutzer	3
Mindestzeit zwischen Kennwortänderungen	1 Tag
Maximaler Zeitraum zwischen Kennwortänderungen	60 Tage
Sind Kennwörter für Konten erforderlich?	ja
Wann kann ein Kennwort erneut verwendet werden?	Nach 5 unterschiedlichen Kennwörtern
Dauer der möglichen Inaktivität, bis eine erneute Anmeldung erforderlich ist	Inaktivität für 15 Minuten
Verzögerung zwischen fehlgeschlagenen Anmeldeversuchen	4 Sekunden

Die Dateien `/etc/pam.d/system-auth` und `/etc/login.defs` werden beim Festlegen der Standardrichtlinien für Cyber Hygiene geändert.

Diese Einstellungen entsprechen den Mindestanforderungen für angemessene Sicherheitsverfahren. Sie sollten diese Einstellungen so ändern, dass sie den Sicherheitsrichtlinien Ihrer Organisation entsprechen. Für folgende Bereiche können Sie die Standardeinstellungen wie folgt ändern:

- Bei der Standardkonfiguration wird die Mindestlänge des Kennworts auf 8 Zeichen festgelegt. Best Practices für sichere Systeme sehen in der Regel sichere Kennwörter mit mindestens 14 Zeichen vor.
- Der maximale Zeitraum für die nächste Kennwortänderung sollte auf einen Wert festgelegt werden, der für Ihre Organisation geeignet ist. Dies wird im Parameter **`inactive`** in der Datei `/etc/shadow` festgelegt. Der Benutzer wird dann am festgelegten Zeitpunkt zum Ändern des Kennworts für die Anmeldung aufgefordert. Wenn der Benutzer das Kennwort nicht ändert, muss das Kennwort von einem Benutzer mit den entsprechenden Berechtigungen zurückgesetzt werden. Ob der in der Datei `/etc/shadow` festgelegte Wert verwendet wird, hängt von der Standardaktion ab, die in der Datei `/etc/default/useradd` festgelegt ist. Wenn die Datei `/etc/default/useradd` den Wert "-1" festlegt, läuft das Kennwort nicht ab. Wenn `/etc/default/useradd` den Wert "0" festlegt, wird der Account gesperrt. Wenn in der Datei `/etc/default/useradd` ein anderer Wert definiert wird, wird der Parameterwert **`inactive`** in `/etc/shadow` für den Ablauf des Kennworts verwendet.
- Es sollten Regeln in Bezug auf die Komplexität und den Inhalt von Kennwörtern erstellt und gemäß der Sicherheitsrichtlinie des Unternehmens implementiert werden.

Weitere Informationen zur Verwaltung von Kennwortrichtlinien finden Sie in der Linux-Dokumentation.

Inaktivierte Linux-Services

Cyber Hygiene inaktiviert oder deinstalliert gefährdete Linux-Services. Diese Services ermöglichen einen Systemzugriff und sollten nur gestartet oder installiert werden, wenn sie benötigt werden.

Die folgenden Linux-Services (daemons) werden standardmäßig nicht gestartet. Sie können bei Bedarf gestartet werden.

- inetd/xinetd
- portmap
- avahi-daemon
- bluetooth
- cups
- hidd
- isdn
- rhnsd
- canna
- pcmcia
- ypbind
- autofs
- smartd
- netfs
- snmpd
- nfs
- samba

Diese Services können mithilfe des Befehls **service** *Servicename* **start** gestartet werden.

Anmerkung: Wenn sie nicht ordnungsgemäß konfiguriert sind, können diese Services beeinträchtigt werden und unbefugten Zugriff zum System ermöglichen. Aus diesen Gründen der Systemsicherheit werden sie standardmäßig nicht gestartet.

Die folgenden Linux-Services wurden entfernt. Sie können bei Bedarf mit den Befehlen **rpm** oder **yum** neu installiert werden. Mit dem Befehl **yum install httpd** wird z. B. das HTTP-Daemonpaket installiert.

- tcpdump
- sendmail
- squid
- vnc-server
- httpd
- mod_python
- mod_perl
- mod_ssl
- webalizer
- httpd-manual

Anmerkung: Diese Services wurden von Linux entfernt, weil sie ein hohes Risikopotenzial für die Sicherheit in Serverumgebungen haben.

Entfernte Benutzer-IDs

Eine standardmäßige Linux-Installation enthält eine Reihe von Benutzer-IDs, die in einer sicheren Produktionsumgebung nicht wünschenswert sind. Cyber Hygiene entfernt diese Benutzer-IDs aus der Linux-Benutzerregistry und aus der Datei `/etc/passwd`. Die dazugehörigen Ausgangsverzeichnisse werden ebenfalls entfernt.

Die folgenden Benutzer-IDs wurden gelöscht und können bei Bedarf erneut erstellt werden.

- games
- news
- ftp
- halt
- shutdown
- reboot
- who
- gopher
- lp
- rpcuser
- uucp

Wenn diese Benutzer-IDs erforderlich sind, können standardmäßige Linux-Administrationsverfahren verwendet werden, um sie zu erstellen.

Prüfungsvorgaben

Die Standardprüfung in Linux ist minimal, da die Prüfungsdateien schnell größer werden können. Wenn jedoch die Sicherheit ein wichtiger Faktor ist, ist eine zusätzliche Prüfung unerlässlich, um bestimmen zu können, was bei einem Vorfall passiert. Scripts von Cyber Hygiene fügen für alle Ausführungsebenen von Linux zusätzliche Prüfungsvorgaben hinzu. Ereignisse, die mit diesen Vorgaben übereinstimmen, werden in den standardmäßigen Systemprotokolldateien protokolliert.

Die folgenden Linux-Prüfungsvorgaben werden hinzugefügt und können bei Bedarf geändert werden.

- Fehlgeschlagene Versuche, auf Programme und Dateien zuzugreifen
- Löschen von Programmen und Dateien
- Administrative und sicherheitsbezogene Aktionen sowie Aktionen, für die eine Berechtigung erforderlich ist
- Änderungen der Zugriffssteuerungsberechtigung

Es ist ein bewährtes Sicherheitsverfahren, über gute Prüfprotokolle zu verfügen. Wenn aus irgendeinem Grund die von Cyber Hygiene definierte Prüfung geändert werden muss, müssen die Dateien `/etc/audit/auditd.conf` und `/etc/audit/audit.rules` entsprechend geändert werden. Cyber Hygiene aktiviert die Prüfung aller fünf Laufzeitebenen von Red Hat Enterprise Linux.

Berechtigungen für Dateien und Verzeichnisse

Cyber Hygiene ändert vorhandene Datei- und Verzeichnisberechtigungen, um die Best Practices in Bezug auf die Sicherheit zu erfüllen.

Folgende Änderungen der Berechtigungen für Dateien und Verzeichnisse wurden von Cyber Hygiene durchgeführt:

Beschränkung von Systemscripts

Auf sensible Scripts des Sicherheitssystems kann von Benutzern ohne die entsprechenden Berechtigungen nicht zugegriffen werden.

Entfernung der globalen Schreibberechtigung

Benutzer können nicht an Verzeichnisse schreiben, die nicht allgemein zugänglich sind. Anwendungen und Benutzer, die Dateien und Verzeichnisse ändern müssen, müssen Berechtigungsinhaber oder ein Mitglied der Berechtigungsgruppe für die Datei oder das Verzeichnis sein.

Entfernung der globalen Schreib- und Ausführungsberechtigung

Die globalen Lese- und Ausführungsberechtigungen werden für viele Dateien und Verzeichnisse entfernt. Diese Berechtigungen werden insbesondere von Benutzerausgangsverzeichnissen entfernt. Anwendungen und Benutzer, die Dateien lesen und ausführen müssen, müssen Berechtigungsinhaber oder ein Mitglied der Berechtigungsgruppe für die Datei oder das Verzeichnis sein.

Weitere Änderungen

Cyber Hygiene nimmt weitere Änderungen vor, um gegen Sicherheitsrisiken vorzugehen.

Befehl 'tch programs - `at`'

Um unbefugte Benutzer daran zu hindern, den Befehl **`at`** zu verwenden, um zu einer bestimmten Zeit Stapelverarbeitungsprogramme auszuführen, löscht Cyber Hygiene die Datei `at.deny` und erstellt eine leere Datei `at.allow`.

Die Datei `at.allow` definiert die Benutzer, die den Befehl **`at`** ausführen dürfen. Die Datei `at.allow`, die keine Benutzer-IDs enthält, setzt voraus, dass keine anderen Benutzer als die System-IDs mit Berechtigung den Befehl **`at`** ausführen dürfen. Wenn die Datei `at.deny` vorhanden ist, die explizit die Benutzer definiert, die den Befehl**`at`** nicht verwenden dürfen, und wenn die Datei `at.allow` nicht vorhanden ist, dann dürfen alle Benutzer, außer die Benutzer in der Datei `at.deny`, den Befehl **`at`** ausführen. Wenn keine der beiden Dateien vorhanden ist, darf nur der Superuser den Befehl **`at`** ausführen.

Red Hat Enterprise Linux ist standardmäßig so konfiguriert, dass Benutzer den Befehl **`at`** ausführen dürfen.

Befehl 'Batch programs - `cron`'

Benutzern ohne Administratorberechtigung ist es nicht erlaubt, den Befehl **`cron`** auszuführen, um Stapelverarbeitungsprogramme zu planen.

Strg-Alt-Entf

Die Tastenkombination Strg-Alt-Entf ist inaktiviert, damit sie nicht zum Abschalten des Systems verwendet werden kann.

Korrekturtools

IBM Intelligent Operations Center Cyber Hygiene bietet Korrekturtools, um Schwachstellen im installierten IBM Intelligent Operations Center-System zu beheben.

Korrekturtools werden ausgeführt, wenn Cyber Hygiene nach Abschluss der IBM Intelligent Operations Center-Installation ausgeführt wird. Diese Tools können auch ausgeführt werden, wenn das System aktiv ist, um Schwachstellen zu finden und zu beheben. Solche Schwachstellen entstehen, wenn andere Produkte auf Servern installiert sind oder wenn das System verwendet wird.

Schwachstellenscanner

Der Scanner besteht aus Scripts, die das IBM Intelligent Operations Center-System überprüfen und Schwachstellen identifizieren. Der Scanner identifiziert beispielsweise Verzeichnisse mit Schreibberechtigungen für jeden Benutzer.

Der Scanner erstellt eine Ergebnisdatei, die von den Korrekturscripts verwendet wird. Diese Ergebnisdatei listet entdeckte Schwachstellen im IBM Intelligent Operations Center-System auf.

Die Scanner-Scripts ändern das IBM Intelligent Operations Center-System nicht, sondern identifiziert nur Schwachstellen. Der Scanner kann nach der Korrektur verwendet werden, um die Änderungen der Korrekturscripts zu prüfen.

Korrekturscripts für Schwachstellen

Cyber Hygiene besitzt drei verschiedene Korrekturscripts:

- Scripts, die Konfigurationsänderungen vornehmen, die nicht gescannt werden müssen, die auf einfache Weise wieder rückgängig gemacht werden können oder die sich nicht erheblich auf die Laufzeit des Systems auswirken. Beispiel: Änderung der Standard-Dateizugriffsberechtigung auf die Man-Pages zu 644.
- Ein Script zum Inaktivieren der Remote-Anmeldung mit dem `root`-Account.
- Ein Script, dass die Ergebnisdatei verarbeitet, die vom Scanner erstellt wurde, und identifizierte Schwachstellen behebt.

  Gehen Sie bei der Verwendung dieses Scripts vorsichtig vor, wenn zusätzliche Produkte installiert sind. Einige Produkte benötigen weniger strenge Einstellungen, daher können Störungen auftreten, wenn diese Scripts ausgeführt werden. Überprüfen Sie die Ergebnisdateien, die von den Scannerscripts erstellt wurden, auf potenzielle Risiken, bevor Sie Korrekturscripts ausführen.

Korrekturprotokolle

Scanning- und Korrekturscripts protokollieren ihre Aktionen in vier Protokolldateien auf jedem IBM Intelligent Operations Center-Server. Diese Protokolle befinden sich im Verzeichnis `/var/BA15/CH/results`. In den Unterverzeichnissen sind Arbeitskopien der Scan- und Korrekturergebnisse enthalten.

Der Scanner wird zwei Mal ausgeführt: ein Mal zum Korrigieren von Schwachstellen und ein zweites Mal zum Protokollieren von nicht durchgeführten Korrekturen. Das Protokoll der zweiten Ausführung kann vom Administrator verwendet werden, um zu bestimmen, ob eine manuelle Korrektur notwendig ist.

Dokumentation von Cyber Hygiene

Es ist Dokumentation verfügbar, um dem Kunden bei der Bewertung der am installierten IBM Intelligent Operations Center-System vorgenommenen Änderungen zu helfen. Diese Dokumentation hilft bei der Zertifizierung und Akkreditierung von Systemen für den Produktionseinsatz.

Die Dokumentation umfasst einen Überblick über die Gesamtstrategie von Cyber Hygiene, die Begründung für die Implementierung bestimmter Standards und eine Tabelle, die den Status jeder durch die DISA markierten Schwachstelle dokumentiert. Die Tabelle kann bei Bewertungen der Produktsicherheit verwendet werden.

Zugehörige Informationen:


Implementierung von Cyber Hygiene in IBM Intelligent Operations Center 1.5

Kapitel 4. Integration der Lösung

Produkte und Services können mit dem IBM Intelligent Operations Center mit Daten, die zu Ereignissen in Beziehung stehen, integriert werden.

Für Ereignisdaten, die an das IBM Intelligent Operations Center übertragen werden, können Common Alerting Protocol oder andere Protokolle verwendet werden.

Diese Ereignisse können zu KPIs (Key Performance Indicators), die vom IBM Intelligent Operations Center überwacht werden, in Beziehung stehen. Ereignisse im IBM Intelligent Operations Center können auch zu Standard Operating Procedures und zu verfügbaren Ressourcen in Beziehung stehen. Die Lösung stellt einen Berichtsadministration-Service bereit, sodass Sie aktuelle Berichte und Zusammenfassungen für Ihre Ereignisdaten erstellen können.

Beispiele integrierbarer Systeme

Produkte und Services können mit dem IBM Intelligent Operations Center integriert werden.

Zu den Beispielen für Systeme und Services gehören folgende:

- Systeme, die über öffentliche Sicherheitsthemen berichten.
- Systeme, die über Verkehrsereignisse berichten.
- Systeme, die über Wasserqualität und -verwendung berichten.
- Systeme, die Daten zu Ausfallzeiten und zum Status zugehöriger Arbeitsaufträge liefern.

Diese Systeme müssen in der Lage sein, mit dem IBM Intelligent Operations Center zu kommunizieren und Ereignisse und Messwerte im unterstützten Protokoll an die IBM Intelligent Operations Center-Warteschlagen für eingehende Ereignisse zu senden.

Zugehörige Konzepte:

„Die Warteschlange für eingehende Ereignisse für das IBM Intelligent Operations Center verwenden" auf Seite 106
CAP-Ereignisse können im IBM Intelligent Operations Center veröffentlicht werden, indem sie an die eingeschlossene WebSphere Message Broker-Instanz übertragen werden.

„Integration mit dem Common Alerting Protocol" auf Seite 99
Das Common Alerting Protocol (CAP) wird verwendet, um Ereignisdaten zwischen dem IBM Intelligent Operations Center und externen Systemen auszutauschen.

Integrationspunkte und -protokolle

Andere Systeme können über die IBM Intelligent Operations Center-Services und -Richtlinien mit der Lösung integriert werden. Daten können im CAP-Format (Common Alerting Protocol) empfangen werden; andere Protokolle werden ebenfalls unterstützt.

Ereignisse und KPIs

Das IBM Intelligent Operations Center verarbeitet Ereignisse und KPIs (Key Performance Indicators), um zu bestimmen, wie Informationen angezeigt werden.

Andere Produkte und Services können mit dem IBM Intelligent Operations Center über den Nachrichtenbus-Service integriert werden. KPIs werden vom Geschäftsüberwachungsservice überwacht.

Ereignisse werden vom IBM Intelligent Operations Center empfangen. Diese Ereignisse können in einem Details-Portlet angezeigt werden und können sich auf die Anzeige in Kartenportlets auswirken.

Mit der KPI-Definition wird festgelegt, wie KPIs in Status- und Key Performance Indicator - Drilldown-Portlets angezeigt werden. Mit der KPI-Definition kann auch bestimmt werden, wie Informationen zu Ereignissen angezeigt werden. Beispiel: Wenn ein KPI-Schwellenwert überschritten wird, wird das Ereignis möglicherweise mit einer höheren Dringlichkeit oder einem höheren Schweregrad markiert. Ereignisse ohne entsprechende KPI-Definitionen werden gemäß den zu dem Ereignis empfangenen Informationen angezeigt.

Weitere Informationen zu Erstellung und Integration von KPIs erhalten Sie über den Link am Ende dieses Themas.

Zugehörige Konzepte:

„KPIs erstellen und integrieren" auf Seite 116
KPI-Modelle (Key Performance Indicator) können mit einem Entwicklungstoolkit zur Geschäftsüberwachung und einem KPI-Managementportlet erstellt und geändert werden.

Richtlinie für KPI-Aktualisierungen

Die IBM Intelligent Operations Center-Richtlinie bestimmt, ob ein eingehendes Ereignis eine KPI-Ereignisaktualisierung ist, sendet es zur Verarbeitung, um in Abhängigkeit von den Parametern eine KPI-Aktualisierung oder einen Alert zu generieren. Ein KPI-Ereignis wird von `<code>KPI</code>` im Alertblock des XML-Codes für Common Alerting Protocol bestimmt.

Wenn das Ereignis als KPI-Aktualisierung bestätigt wird, prüft die Richtlinie die KPI-Parameter und generiert einen XML-Code für das KPI-Ereignis, der an den IBM WebSphere Business Monitor zur Verarbeitung gesendet wird.

Die folgende Tabelle enthält ein Beispiel für die Aktualisierung eines KPI-Ereignisses.

Tabelle 29. KPI-Beispielereigniseigenschaften

Eigenschaft	Wert
Absender	security@rtp.city.gov
Ereignistyp	Reaktionszeit auf Verbrechen
Ereignisstatus	Tatsächlich - umsetzbar durch alle Zielempfänger
Ereignisbereich	Öffentlich - zur Verbreitung an nicht beschränkte Zielgruppen
Kategorie	Sicherheit
Schweregrad	Schwerwiegend
Gewissheit	Wahrscheinlich
Dringlichkeit	Sofort
Nachrichtentyp	Alert - anfängliche Informationen, die von den zielgruppenspezifischen Empfängern beachtet werden müssen
Beschreibung	Einbruch
Sendedatum und -uhrzeit	2012-02-17T17:06:00+01:00
Startdatum/-uhrzeit	2012-02-16T15:47:00+01:00
Datum/Uhrzeit der Reaktion	2012-02-17T17:06:00+01:00

In der folgenden Tabellen sind die KPI-Beispielparameter enthalten, die der KPI-Ereignisaktualisierung in Tabelle 29 zugeordnet sind.

Tabelle 30. KPI-Beispielereignisparameter

Parameter	Wert
Berichtsnummer	1111
Bezirk	Bezirk 1
Reaktion	2011-02-15T15:05:07-05:00

Zugehörige Konzepte:

„Status" auf Seite 306
Mit dem Portlet "Status" können Sie den Status von KPIs einer einzelnen Einrichtung oder mehrerer Einrichtungen anzeigen.

„Benachrichtigungen" auf Seite 302
Mit dem Portlet "Benachrichtigungen" können Sie Alertnachrichten sowie Details zu diesen Nachrichten anzeigen.

Integration mit dem Common Alerting Protocol

Das Common Alerting Protocol (CAP) wird verwendet, um Ereignisdaten zwischen dem IBM Intelligent Operations Center und externen Systemen auszutauschen.

Das CAP ist ein generisches Format für den Austausch von Notfall-Alerts und öffentlichen Warnungen in verschiedenen Netzen. Es stellt ein offenes, nicht proprietäres digitales Nachrichtenformat für alle Arten von Alerts und Benachrichtigungen bereit. Das CAP ist mit neu entstehenden Verfahren, wie z. B. Web-Services, kompatibel und bietet gleichzeitig ein erweitertes Leistungsspektrum. Zu diesem Leistungsspektrum gehört Folgendes:

- Flexible geografische Zielbestimmung mit Breitengrad- und Längengradformen und anderen dreidimensionalen Geodarstellungen
- Mehrsprachiges, an ein breites Publikum gerichtetes Messaging
- In Phasen unterteilte und verzögerte effektive Zeiten und Ablaufdaten
- Erweiterte Nachrichtenaktualisierungs- und Abbruchfunktionen
- Vorlagenunterstützung für das Framing von vollständigen und effektiven Warnungen
- Digitale Verschlüsselung und Signaturkompatibilität
- Digitale Bilder und Audiofunktionen

Ereignisse sind eigenständige Datennachrichten, die von allen Komponenten gesendet oder verarbeitet werden können. Ereignisse können für Themenwarteschlangen veröffentlicht werden und von allen potenziell interessierten IT-Systemen, die über ein Abonnement verfügen, gelesen werden. Das CAP unterstützt die Standardisierung von Ereignisinhalten, sodass mehrere Domänen Ereignisse in einem gemeinsamen Format mit gemeinsamen Konventionen senden und empfangen können. Der Standard definiert die obligatorischen und optionalen Felder im Ereignissatz und die zulässigen Werte für diese Felder. Das Ereignisverarbeitungsmanagement kann zwischen traditionellen Formaten und dem Standardformat vermitteln. Zusätzlich zu Notfallsituationen kann das CAP für die Verarbeitung von alltäglichen Operationen erweitert werden.

Ereignisse müssen mindestens Folgendes enthalten:

- Eine eindeutige Ereignis-ID, die Folgendes enthält:
  - Den Absender (System oder Person)
  - Organisation, die das Ereignis sendet
  - Seriennummer im sendenden System
  - Zeitmarke der Ereigniserstellung
- Informationen, mit denen Empfänger Antworten definieren und priorisieren können:
  - Dringlichkeit – wie schnell Empfänger auf den Alert reagieren sollten

  - Grad der Bedrohung für Leben und Eigentum
  - Wahrscheinlichkeit – eine Wahrscheinlichkeit, die von 100 % (das Ereignis wurde beobachtet) bis 0 % reicht (das Ereignis wird erwartungsgemäß nicht auftreten)
  - Prognostizierte Zeit für Ereignisse, die möglicherweise in der Zukunft stattfinden
  - Dauer von Ereignissen, die zuvor gemeldet wurden und deren Fortsetzung gemeldet wird
  - Voraussichtliche Dauer von Ereignissen, die eine Situation darstellen, die nicht umgehend korrigiert werden kann
  - Empfohlene oder in Auftrag gegebene Aktionen und Anweisungen
- Informationen, die die Korrelation des Ereignisses ermöglichen:
  - Semantikmodellverweise für Stadt (falls vorhanden)
  - Geokoordinaten
  - Verweis auf vorausgesetztes Ereignis oder ein auslösendes Ereignis
  - Eindeutige Asset-IDs für alle Beteiligten
- Menschenlesbare Beschreibungen:
  - Standortbeschreibung
  - Aktivitätenbeschreibung

Mit dem CAP kann der Datenaustausch für Ereignisse minimiert werden. Da Ereignisse in XML formatiert sind, kann das Datenformat von einer Vielzahl von Systemen geschrieben und gelesen werden. Damit wird der Austausch von unnützen Daten oder Daten, die zu gefährlichen Verwirrungen führen, vermieden.

Das IBM Intelligent Operations Center stellt einen permanenten Speicher für CAP-Alerts und eine Standardschnittstelle für die Darstellung bereit.

Während die gesamte CAP-Struktur vom IBM Intelligent Operations Center akzeptiert wird, werden nur einige Daten vom IBM Intelligent Operations Center für die Berechnung der KPIs (Key Performance Indicators) verwendet.

Das IBM Intelligent Operations Center verwendet den WebSphere Message Broker, um Ereignisse mit dem CAP zu integrieren.

Das IBM Intelligent Operations Center unterstützt OASIS Common Alerting Protocol Version 1.2.

Zugehörige Konzepte:

„CAP für KPI-Ereignisse verwenden" auf Seite 103
Der WebSphere Message Broker, der als Teil vom IBM Intelligent Operations Center bereitgestellt wird, akzeptiert CAP-Ereignisnachrichten und verwendet die Dateien in KPI-Berechnungen (Key Performance Indicator).

„CAP für Nicht-KPI-Ereignisse verwenden" auf Seite 105
CAP-Daten können auch verwendet werden, um Daten zu Ereignissen bereitzustellen, die keinen KPI-Berechnungen zugeordnet sind.

Zugehörige Informationen:

OASIS Common Alerting Protocol Version 1.2

CAP-Struktur

Jede CAP-Alertnachricht besteht aus einem Segment des Typs `<Alert>`, das mindestens ein `<info>`-Segment enthalten kann. Jedes Segment des Typs `<info>` kann mindestens ein `<area>`-Segment enthalten. In den meisten Fällen enthalten CAP-Nachrichten mit einem Nachrichtentyp (`<msgType>`) mit einem Wert von *Alert* mindestens ein `<info>`-Segment.

Die wichtigsten Nachrichtenelemente sind:

- <alert>

  Das Segment <alert> stellt Basisinformationen über die aktuelle Nachricht bereit, d. h. ihren Zweck, ihre Quelle und ihren Status. Es umfasst außerdem eine eindeutige Kennung für die Nachricht und Links zu allen anderen verwandten Nachrichten. Ein Segment des Typs <alert> kann nur für Nachrichtenbestätigungen und -abbrüche oder andere Systemfunktionen verwendet werden. Allerdings enthalten die meisten Segmente des Typs alert mindestens ein<info>-Element.
- <info>

  Das Segment <info> beschreibt ein voraussichtliches oder tatsächliches Ereignis hinsichtlich der Dringlichkeit (die verfügbare Vorbereitungszeit), des Schweregrades (die Intensität der Auswirkung) und der Gewissheit (Zuverlässigkeit der Beobachtung oder der Voraussage). Es stellt außerdem Beschreibungen des jeweiligen Ereignisses nach Kategorien oder in Textform bereit. Das Segment <info> bietet möglicherweise auch Anweisungen für eine angemessene Antwort der Nachrichtenempfänger und weitere Angaben, wie z. B. die Dauer der Gefahr, technische Parameter, Kontaktinformationen und Links zu weiteren Informationsquellen. Es können mehrere Segmente des Typs <info> verwendet werden, um verschiedene Parameter, wie z. B. unterschiedliche Wahrscheinlichkeits- oder Intensitätsbereiche, zu beschreiben oder um die Informationen in mehreren Sprachen bereitzustellen.
- <resource>

  Das Segment <resource> stellt einen optionalen Verweis auf zusätzliche Informationen bereit, die in Beziehung zu dem Segment <info> stehen. Es verweist möglicherweise auf eine digitale Ressource wie eine Bild- oder Audiodatei.
- <area>

  Das Segment <area> beschreibt einen geografischen Bereich, auf den das Segment <info> Anwendung findet. Beschreibungen in Textform und codierte Beschreibungen (z. B. Postleitzahlen) werden unterstützt, aber die bevorzugten Darstellungen verwenden geografisch-räumliche Formen, Vielecke und Kreise sowie eine Höhe oder einen Höhenbereich, der in standardisierten Begriffen von Breitengrad, Längengrad und geografischer Höhe ausgedrückt wird und mit einem bestimmten geografisch-räumlichen Bezugspunkt übereinstimmt.

Zugehörige Konzepte:

„CAP für KPI-Ereignisse verwenden" auf Seite 103
Der WebSphere Message Broker, der als Teil vom IBM Intelligent Operations Center bereitgestellt wird, akzeptiert CAP-Ereignisnachrichten und verwendet die Dateien in KPI-Berechnungen (Key Performance Indicator).

„CAP für Nicht-KPI-Ereignisse verwenden" auf Seite 105
CAP-Daten können auch verwendet werden, um Daten zu Ereignissen bereitzustellen, die keinen KPI-Berechnungen zugeordnet sind.

Ereignistypen

IBM Intelligent Operations Center unterstützt mehrere CAP-Ereignistypen.

Tatsächliches/vorhergesagtes Ereignis

Tatsächliche/vorhergesagte Ereignisnachrichten sind nicht angeforderte Nachrichten, die von diversen Domänen aufgrund von Unregelmäßigkeiten oder Ausnahmebedingungen gesendet werden. Diese Nachrichten decken auch KPI-Verstöße ab, wenn ein Ereignis erstellt wird.

Bestätigung (Acknowledgment)

Eine Bestätigung ist eine CAP-Nachricht mit den folgenden Feldwerten im Element <alert>:

- Der Wert für <msgType> ist auf **ACK** gesetzt, was bedeutet, dass der Sender den Erhalt und die Abnahme der in <references> angegebenen Nachrichten bestätigt hat.
- Das Feld <references> enthält die erweiterten Nachrichtenkennungen (im Format sender, identifier, sent, d. h. Sender, Kennung, gesendet) einer früheren CAP-Nachricht oder von Nachrichten, auf die durch die Bestätigung verwiesen wird.

•

Anmerkung: Das Element <info> ist für eine Bestätigung optional.

Antwort (Response)

Eine Antwort ist eine CAP-Nachricht mit den folgenden Feldwerten im Element <alert>:

- Der Wert für <msgType> ist **Alert**.
- Der Wert für <note> ist **Response**.
- Das Element <references> muss die Kennungen der CAP-Nachricht enthalten, auf die dies eine Antwort ist.

Wenn z. B. ein Stadtnetzbetreiber eine **Empfehlung für Spannungsabfall** an diverse Domänen sendet, senden diese Domänen eine Antwort an die Empfehlung zurück, nachdem sie eine Abhängigkeitsanalyse für ihre individuellen Funktionen durchgeführt haben.

Vorfall

Vorfälle werden verwendet, um mehrere Nachrichten zu sortieren, die sich auf unterschiedliche Aspekte desselben Vorfalls beziehen. CAP-Nachrichten des Typs Vorfall dienen als Behälter für alle Ereignisse in Verbindung zu einem bestimmten Vorfall. Diese Ereignisse können sich in verschiedenen Domänen befinden.

Eine Empfehlung wird zu einem Vorfall hochgestuft, wenn Domänen Antworten an die Empfehlung zurücksenden, in denen angegeben wird, dass Auswirkungen auf mehrere Domänen eine koordinierte Aktion erfordern. Das Element <incident> (Vorfall) ist in allen verwandten Ereignissen mit dem Wert <identifier> des Ereignisses vom Typ Vorfall belegt. Verwandte Ereignisse sind Ereignisse, bei denen der Wert <references> mit dem Wert <identifier> des Ereignisses Vorfall übereinstimmt.

Ein Vorfall ist eine CAP-Nachricht mit den folgenden Feldwerten im Element <alert>:

- Der Wert für <msgType> ist **Alert**.
- Der Wert für <note> ist **Incident**.
- Das Element <references> muss die Kennungen der CAP-Nachricht enthalten, die das dem Ereignis übergeordnete Element (die eigentliche Ursache) ist.
- Das Element <incidents> muss seine eigene Kennung enthalten.

Update

Eine Aktualisierung ist eine CAP-Nachricht mit den folgenden Feldwerten im Element <alert>:

- Das Element <msgType> ist auf **update** eingestellt. Das bedeutet, dass dieses Update die vorherigen, im Element <references> angegebenen Nachrichten ersetzt.
- Das Element <references> enthält die erweiterten Nachrichtenkennungen (im Format sender,identifier,sent) von einer früheren CAP-Nachricht oder von Nachrichten, auf die durch das Update verwiesen wird.

Abbrechen (Cancel)

Abbrechen ist eine CAP-Nachricht mit den folgenden Feldwerten im Element <alert>:

- Das Element <msgType> ist auf **Cancel** eingestellt. Das bedeutet, dass diese Nachricht die vorherigen, im Element <references> angegebenen Nachrichten abbricht.
- Das Element <references> enthält die erweiterten Nachrichtenkennungen (im Format sender,identifier,sent) von einer früheren CAP-Nachricht oder von Nachrichten, auf die durch diesen Abbruch verwiesen wird.

- Das Element <note> enthält eine Erklärung dazu, warum oder wie dieser Alert behoben wird.

Zugehörige Informationen:

OASIS Common Alerting Protocol Version 1.2

CAP für KPI-Ereignisse verwenden

Der WebSphere Message Broker, der als Teil vom IBM Intelligent Operations Center bereitgestellt wird, akzeptiert CAP-Ereignisnachrichten und verwendet die Dateien in KPI-Berechnungen (Key Performance Indicator).

Tabelle 31 listet die in KPI-Berechnungen verwendeten Datenelemente auf:

Tabelle 31. CAP-Elemente, die in IBM Intelligent Operations Center-KPI-Berechnungen verwendet werden

Erforderlich oder optional	Datenelement (normativ)	Beschreibung
Erforderlich	Message_ID (ID)	Eindeutige Nachrichten-ID
Erforderlich	Sender_ID (Sender)	Eindeutige Sender-ID
Erforderlich	SentDateTime (Gesendet)	Datum und Uhrzeit, zu der die Nachricht gesendet wurde Beispiel: 2011-02-07T 16:49:00-05:00 enthält das Datum und die Uhrzeit, an dem bzw. zu der eine Nachricht gesendet wurde. Die letzten sechs Zeichen geben die Zeitzone des CAP-Ereignisses in Bezug zur Greenwich Mean Time (GMT) an. In diesem Fall hat das Ereignis um 16:49:00 stattgefunden, zur GMT minus 5 Stunden, was der Eastern Standard Time (EST) entspricht. Dieser Code bedeutet, dass das Ereignis beim Anzeigen von EST in die Zeitzone des Benutzers konvertiert wird. Wenn Sie Ihre CAP-Ereignisse anstatt dessen in GMT codieren möchten, ändern Sie das Suffix in -00:00, wie im folgenden Beispiel: 2011-02-07T 16:49:00-00:00.
Erforderlich	MessageStatus (Status)	Für den Status der Nachricht kann eine der folgenden Optionen angegeben werden: • Actual • Exercise • System • Test • Draft
Erforderlich	MessageType (Nachrichtentyp)	Für den Typ der Nachricht kann eine der folgenden Optionen angegebenen werden: • Alert • Update • Cancel • Ack • Error
Optional	Source (Quelle)	Quelle der Nachricht
Erforderlich	Scope (Bereich)	Enthält den Wert Public
Erforderlich	Code (Code)	Enthält den Wert KPI, um dieses Ereignis aus der Ereignisse-Portletliste auszublenden.

Tabelle 31. CAP-Elemente, die in IBM Intelligent Operations Center-KPI-Berechnungen verwendet werden (Forts.)

Erforderlich oder optional	**Datenelement (normativ)**	**Beschreibung**
Erforderlich	`EventCategory` (Kategorie)	Eine der folgenden Optionen: • `Geo` • `Met` • `Safety` • `Security` • `Rescue` • `Fire` • `Health` • `Env` • `Transport` • `Infra` • `CBRNE` • `Other`
Erforderlich	`EventType` (Ereignis)	Beschreibung des Ereignisses oder des KPI. Beispiel: `Police_Department_Budget`
Erforderlich	`Urgency` (Dringlichkeit)	Eine der folgenden Optionen: • `Immediate` • `Expected` • `Future` • `Past` • `Unknown`
Erforderlich	`Severity` (Schweregrad)	Der Schweregrad wird mit einer der folgenden Optionen angegeben: • `Extreme` • `Severe` • `Moderate` • `Minor` • `Unknown`
Erforderlich	`Certainty` (Wahrscheinlichkeit)	Die Wahrscheinlichkeit wird mit einer der folgenden Optionen angegeben: • `Observed` • `Likely` • `Possible` • `Unlikely` • `Unknown`
Optional	`EventCode` (Ereigniscode)	Name/Wert-Paare für die Ereignistypisierung.
Optional	`OnsetDateType` (Start)	Startdatum und -uhrzeit des Ereignisses Beispiel: `2011-02-08T16:49:00-05:00`
Optional	`SenderName` (Sendername)	Name der Entität, die den Alert gestartet hat. Beispiel: `Police Department`
Optional	`EventDescription` (Beschreibung)	Ausführliche Beschreibung des Ereignisses oder des KPI

Tabelle 31. CAP-Elemente, die in IBM Intelligent Operations Center-KPI-Berechnungen verwendet werden (Forts.)

Erforderlich oder optional	Datenelement (normativ)	Beschreibung
Optional	`Parameter` (Parameter)	Zusätzliche Daten, die dem Ereignis oder KPI zugeordnet sind.
Optional	`AreaGeocode` (Geocode)	Ein Feld, das für die Bereitstellung von Informationen verwendet werden kann, wenn das Ereignis oder der KPI ortsabhängig ist

Weitere Informationen erhalten Sie über den zugehörigen Link am Ende dieses Themas zur OASIS-Common Alerting Protocol-Spezifikation.

Im Folgenden finden Sie einen Beispielcode eines Ereignisberichts zu einem Autounfall.

```
<?xml version="1.0" encoding="UTF-8"?>
<cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:oasis:names:tc:emergency:cap:1.2 CAP-v1.2-os.xsd ">
 <cap:identifier>1112</cap:identifier>
 <cap:sender>Transportation</cap:sender>
 <cap:sent>2011-02-17T15:00:00-05:00</cap:sent>
 <cap:status>Actual</cap:status>
 <cap:msgType>Alert</cap:msgType>
 <cap:scope>Public</cap:scope>
 <cap:code>KPI</cap:code>
 <cap:info>
  <cap:category>Transport</cap:category>
  <cap:event>Traffic_Accident</cap:event>
  <cap:urgency>Unknown</cap:urgency>
  <cap:severity>Extreme</cap:severity>
  <cap:certainty>Unknown</cap:certainty>
  <cap:eventCode>
   <cap:valueName>OwningOrg</cap:valueName>
   <cap:value>Police</cap:value>
  </cap:eventCode>
  <cap:onset>2011-02-17T15:00:00-05:00</cap:onset>
  <cap:senderName>Transportation</cap:senderName>
  <cap:description>Single car crash</cap:description>
  <cap:parameter>
   <cap:valueName>accident number</cap:valueName>
   <cap:value>1112</cap:value>
  </cap:parameter>
 </cap:info>
</cap:alert>
```

Zugehörige Konzepte:

„Benutzerschnittstelle lokalisieren” auf Seite 149
Die Browsereinstellungen bestimmen die Einstellungen für Sprache, Datum und Uhrzeit für die Benutzerschnittstelle des IBM Intelligent Operations Center. Ein Administrator kann die Formate für Datum und Uhrzeit anpassen.

„Bekannte Probleme und Lösungen” auf Seite 347
Dieser Abschnitt enthält eine Liste häufig auftretender Probleme sowie eine Lösung für die einzelnen Punkte.

Zugehörige Informationen:

OASIS Common Alerting Protocol Version 1.2

CAP für Nicht-KPI-Ereignisse verwenden

CAP-Daten können auch verwendet werden, um Daten zu Ereignissen bereitzustellen, die keinen KPI-Berechnungen zugeordnet sind.

Vom IBM Intelligent Operations Center empfangene CAP-Daten, die keinen definierten KPIs zugeordnet sind, werden den Portlets Ereignisse und Karte im IBM Intelligent Operations Center hinzugefügt.

Der folgende Code bezieht sich auf ein Nicht-KPI-Musterereignis. Beachten Sie, dass Sie für Nicht-KPI-Ereignisse den Wert des Tags `code` auf `Event` setzen müssen.

```
<p>
 <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
   <identifier>f30f190c-41fd-431e-ace9-88b725f1a3fc</identifier>
   <sender>TestGenerator</sender>
   <sent>2012-03-26T15:47:24-00:00</sent>
   <status>Actual</status>
   <msgType>Alert</msgType>
   <scope>Public</scope>
   <restriction/>
   <code>Event</code>
   <info>
     <language>en_US</language>
     <category>Infra</category>
     <event>Water Main Break</event>
     <urgency>Immediate</urgency>
     <severity>Moderate</severity>
     <certainty>Observed</certainty>
     <headline>Major water line leak at NW 20th St.</headline>
     <description>Leak is located at the intersection of NW 20th Street and NW 9th Avenue.
     Street flooding starting tooccur. Immediate action required.</description>
     <area>
       <circle>25.79518,-80.21110 0</circle>
     </area>
   </info>
 </alert>
</p>
```

Die Warteschlange für eingehende Ereignisse für das IBM Intelligent Operations Center verwenden

CAP-Ereignisse können im IBM Intelligent Operations Center veröffentlicht werden, indem sie an die eingeschlossene WebSphere Message Broker-Instanz übertragen werden.

Veröffentlichende Clients können so konfiguriert werden, dass sie direkt auf die WebSphere Message Broker-Eingabewarteschlange für CAP-Ereignisse verweisen, oder sie können die auf dem Portalserver definierten WebSphere Application Server-JMS-Ressourcen verwenden. Diese JMS-Ressourcen zeigen auf die WebSphere Message Broker-Warteschlange, die CAP-Ereignisse empfängt. Die folgenden JMS-Ressourcen werden erstellt, wenn das IBM Intelligent Operations Center installiert wird:

- Wartschlangenverbindungsfactory
  - Name: `ioc.mb.con.factory`
  - JNDI-Name: `jms/ioc.mb.con.factory`
- Warteschlange
  - Name: `ioc.cap.in.q`
  - JNDI-Name: `jms/ioc.cap.in.q`

Zugehörige Konzepte:

„KPI-Ereigniskommunikation zwischen IBM WebSphere Business Monitor und IBM Intelligent Operations Center" auf Seite 123
IBM WebSphere Business Monitor kann abgehende Ereignisse von einem Monitoring- oder KPI-Kontext an IBM Intelligent Operations Center senden.

Ereignisse mit dem Publisher-Service erstellen

Sie können Ereignisse an IBM Intelligent Operations Center über Web-Services an den Publisher-Service übertragen.

Sie können Clientanwendungen erstellen, die in eine implementierte Instanz von IBM Intelligent Operations Center integriert werden können. Sie können eine Clientanwendung verwenden, um CAP-Alerts von einer Clientanwendung eines Fremdanbieters an IBM Intelligent Operations Center zu übergeben, indem Sie die von der Dienstprogrammklasse des Publisher-Service und die vom IBM Intelligent Operations Center-Publisher-Servlet bereitgestellten Methoden aufrufen.

Mit den allgemeinen Utility-Klassen entwickeln

Wenn Sie eine Clientanwendung erstellen möchten, die den Publisher-Service aufruft, müssen Sie zuvor die allgemeinen Utility-Klassen einrichten. Nachdem Sie die Entwicklung Ihrer Clientanwendung abgeschlossen haben, exportieren Sie sie als WAR-Datei, die Sie anschließend in WebSphere Application Server importieren.

Informationen zu diesem Vorgang

Verwenden Sie die folgende Prozedur, wenn Sie eine Clientanwendung mit den allgemeinen Utility-Klassen entwickeln möchten:

- Bevor Sie Ihre Clientanwendung entwickeln, fügen Sie die JAR-Dateien `iss_common` und `icu4j-4_4_2` dem Buildpfad des Projekts hinzu. Die JAR-Dateien sind zur Kompilierzeit erforderlich.
- Nachdem Sie die Entwicklung Ihrer Clientanwendung abgeschlossen haben, exportieren Sie sie als WAR-Datei.
- Importieren Sie die WAR-Datei in WebSphere Application Server und konfigurieren Sie sie so, dass sie auf die gemeinsam genutzten Bibliotheken verweist.

Vorgehensweise

1. Suchen Sie die Datei `iss_common.jar` und die Datei `icu4j-4_8_1_1.jar` im Installationsverzeichnis von IBM Intelligent Operations Center (`/opt/IBM/iss/common/lib`).
2. Kopieren Sie die Datei `iss_common.jar` und die Datei `icu4j-4_8_1_1.jar` in ein Verzeichnis auf Ihrer Entwicklungsmaschine.
3. Um die JAR-Dateien dem Buildpfad des Projekts hinzuzufügen, führen Sie in der IBM Intelligent Operations Center-API die folgenden Unterschritte für `iss_common.jar` und `icu4j-4_8_1_1.jar` aus:
   a. Klicken Sie mit der rechten Maustaste auf das **Portletprojekt**.
   b. Klicken Sie auf **Buildpfad** > **Buildpfad konfigurieren**.
   c. Klicken Sie auf die Registerkarte **Bibliotheken** und klicken Sie auf **Externe JARs hinzufügen...**.
   d. Suchen Sie das Verzeichnis, das die JAR-Datei enthält.
   e. Klicken Sie auf die JAR-Datei und anschließend auf **Öffnen**.
4. Wenn Sie die Entwicklung Ihrer Clientanwendung abgeschlossen haben, exportieren Sie sie als WAR-Datei.
5. Verwenden Sie in der Verwaltungskonsole von WebSphere Application Server den Importassistenten, um die WAR-Datei der Clientanwendung zu importieren.
6. Führen Sie folgende Unterschritte aus, um die WAR-Datei so zu konfigurieren, dass sie auf die gemeinsam genutzten Bibliotheken verweist:
   a. Aktivieren Sie in der Verwaltungskonsole von WebSphere Application Server das Kontrollkästchen neben der importierten WAR-Datei und klicken Sie anschließend auf **Aktualisieren**.
   b. Klicken Sie auf **Shared library references** (Verweise für gemeinsam genutzte Bibliotheken).
   c. Aktivieren Sie im Fenster **Shared library references** (Verweise für gemeinsam genutzte Bibliotheken) das Kontrollkästchen **Anwendung**.
   d. Klicken Sie auf **Reference shared libraries** (Verweise für gemeinsam genutzte Bibliotheken).
   e. Verschieben Sie **ISSCommonJars** und **IOCCommonJars** aus der Liste "Verfügbar" in die Liste "Ausgewählt" und klicken Sie anschließend auf **OK**.
   f. Klicken Sie zum Speichern Ihrer Änderungen auf **OK**.

Publisher-Service verwenden

Das Injector-Tool für Publisher-Serviceereignisse wird als Java-Dienstprogramm zur Verfügung gestellt. Sie können eine Clientanwendung erstellen, die XML-Code für CAP an das IBM Intelligent Operations Center übergibt, in dem Sie die vom Publisher-Service bereitgestellten Methoden aufrufen. Sie können auch Benachrichtigungen übergeben.

Der Publisher-Service ist eine Utility-Klasse im Projekt `iss_common_utils`, die in der Datei `iss_common.jar` integriert ist. Der Publisher-Service stellt die statischen Methoden `publishEvent` und `publishNotification` bereit. Bevor Sie Clientanwendungen für den Publisher-Service erstellen, müssen Sie die allgemeinen Utility-Klassen einrichten. Weitere Informationen erhalten Sie über den Link am Ende des Themas.

Um sicherzustellen, dass der Code, der zum Aufrufen des Publisher-Service verwendet wird, Zugriff auf die korrekten Konfigurationen der JMS-Warteschlange hat, müssen Sie ihn auf dem Anwendungsserver implementieren.

Im folgenden finden Sie einen Beispielcode für den Aufruf des Publisher-Service:

```
import com.ibm.iss.common.publisher.Publisher;

String capMessage = request.getParameter(EVENT_TEXT_KEY);

int status = Publisher.publishEvent(capMessage);

if (status == Publisher.STATUS_SUCCESS) {
logger.traceFine(this, methodName, "Event submit request was performed successfully");
}
else if (status == Publisher.STATUS_EXCEPTION_NAMING) {
logger.traceFine(this, methodName, "Error sending CAP Event Message. Requires defining JMS Resources.");
}
else if (status == Publisher.STATUS_EXCEPTION_JMS) {
logger.traceFine(this, methodName, "Error sending CAP Event Message. Failed to connect to JMS resources.");
}
else { //Other error code
logger.traceFine(this, methodName, "Error sending CAP Event Message. Returned status = " + status);
}
```

Wenn Sie das Beispiel-Publisher-Portlet verwenden, brauchen Sie den Code für den Aufruf des Publisher-Service nicht zu erstellen bzw. keine CAP-Nachrichten zu schreiben.

Zugehörige Konzepte:

„Beispiel-Publisher” auf Seite 110
Mit dem Portlet "Beispiel-Publisher" können CAP-Ereignisse (Common Alerting Protocol) in IBM Intelligent Operations Center veröffentlicht werden.

Zugehörige Tasks:

„Mit den allgemeinen Utility-Klassen entwickeln” auf Seite 107
Wenn Sie eine Clientanwendung erstellen möchten, die den Publisher-Service aufruft, müssen Sie zuvor die allgemeinen Utility-Klassen einrichten. Nachdem Sie die Entwicklung Ihrer Clientanwendung abgeschlossen haben, exportieren Sie sie als WAR-Datei, die Sie anschließend in WebSphere Application Server importieren.

Publisher-Servlet verwenden

Das Publisher-Servlet akzeptiert Parameter in POST-Anforderungen zum Veröffentlichen von XML-Code für CAP, zum Erstellen neuer Ereignisse oder zum Erstellen geänderter Ereignisse aus bestehenden Ereignissen oder Vorfällen.

POST-Anforderungen an das Publisher-Servlet senden

Das Publisher-Servlet ruft den Publisher-Service auf, um den XML-Code für CAP in die Warteschlangen zu stellen, die dem IBM Intelligent Operations Center zugeführt werden. Das Publisher-Servlet befindet

sind unter `/ibm/iss/common/rest/publisher`. In der folgenden Tabelle ist veranschaulicht, wie POST-Anforderungen an das Publisher-Servlet gesendet werden.

Tabelle 32. POST-Anforderungen für Publisher-Servlet

Typ des zu veröffentlichenden Ereignisses	**POST-Anforderungscode**
Neues CAP-Ereignis veröffentlichen	`action=publishEvent&source=xml&xml=`*`XML_für_CAP-Ereignis`*
Bestehendes Ereignis ändern	`action=publishEvent&source=existing&id=`*`Ereignis-ID`*
Leeres neues Ereignis veröffentlichen	`action=publishEvent&source=new`

Optionale Parameter

Sie können jeder Veröffentlichungsoption optionale Parameter hinzufügen, indem Sie den folgenden Code an die POST-Anforderung anhängen: `&`*`Parametername=neuer_Wert`*

Die folgenden optionalen Parameter sind verfügbar:

- areaDesc
- category
- certainty
- code
- contact
- description
- event
- headline
- latitude
- longitude
- msgType
- randomize
- randomizeid
- randomizeArea
- randomizeTime
- sender
- senderName
- severity
- status
- urgency

Beispiel: Um ein leeres neues Ereignis zu veröffentlichen und anschließend die Überschrift auf `Traffic` zu setzen, lautet der POST-Anforderungscode wie folgt: `servletURL&action=publishEvent&source=new &headline=Traffic Accident`

Testereignisse erstellen und veröffentlichen

Das IBM Intelligent Operations Center stellt das Portlet "Beispiel-Publisher" und das Portlet "Erstellung von Ereignisscripts" zum Erstellen und Veröffentlichen von Testereignissen bereit.

Zugehörige Konzepte:

„Ereignisse mit dem Publisher-Service erstellen” auf Seite 106
Sie können Ereignisse an IBM Intelligent Operations Center über Web-Services an den Publisher-Service übertragen.

Beispiel-Publisher

Mit dem Portlet "Beispiel-Publisher" können CAP-Ereignisse (Common Alerting Protocol) in IBM Intelligent Operations Center veröffentlicht werden.

Das Portlet "Beispiel-Publisher" ist ein Tool für automatisierte Tests, mit dem Administratoren die Lösung verwalten und überprüfen können. So können Administratoren mit dem Portlet "Beispiel-Publisher" als Clientanwendung die Veröffentlichung von CAP-Nachrichten in IBM Intelligent Operations Center testen. Damit entfällt bei Verwendung des Portlets "Beispiel-Publisher" die Notwendigkeit, Testclientanwendungen manuell zu erstellen.

Ereignisse und Benachrichtigungen erstellen

Starten Sie das Portlet "Beispiel-Publisher", indem Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Demonstration Tools** > **Sample Event Publisher** (Intelligent Operations > Demonstrationstools > Beispiel-Publisher) klicken.

Auf der Registerkarte **Ereignis-CAP** des Portlets "Beispiel-Publisher" können Sie mithilfe eines Formulars Ereignisse mit XML definieren. Beim Senden des Formulars wird das Senden von CAP-Beispielereignissen in das System aktiviert.

Darüber hinaus enthält das Portlet "Beispiel-Publisher" die Registerkarte **Ereignisformular**, über die neue Ereignisse erstellt werden können, wenn keine Bearbeitung des XML-Codes erforderlich ist. Füllen Sie das Formular auf der Registerkarte **Ereignisformular** aus, um die CAP-Ereignisdetails zu senden. Soll ein neues Ereignis auf Basis der Eigenschaften eines bereits vorhandenen Ereignisses erstellt werden, geben Sie im Feld **ID** die CAP-Alert-ID des bereits vorhandenen Ereignisses ein.

Über die Registerkarte **Benachrichtigung** im Portlet "Beispiel-Publisher" kann das Benachrichtigungssubsystem in IBM Intelligent Operations Center getestet werden. Sie können auf dieser Registerkarte ein Formular ausfüllen, um eine Alertbenachrichtigung für angegebene Gruppen zu senden. Im Feld **Gesendet an Gruppen** müssen vorhandene Gruppen angegeben werden (beispielsweise "CityWideOperator" oder "CityWideExecutive"), da im Listenportlet "Benachrichtigungen" nur Alerts angezeigt werden, für die Übereinstimmungen gefunden werden.

Willkürlich ausgewählte Werte

Wenn Sie auf den Registerkarten **Ereignis-CAP** und **Ereignisformular** das Kontrollkästchen **Ereignisse willkürlich auswählen** auswählen, werden die Eigenschaften der vom Portlet veröffentlichten Ereignisse automatisch wie folgt geändert:

- **ID**: Im Portlet wird für jedes Ereignis eine eindeutige ID-Zeichenfolge erstellt, da Ereignis-IDs innerhalb von IBM Intelligent Operations Center eindeutig sein müssen.
- **Timestamp** (Zeitmarke): Das Portlet erhöht für jedes gesendete Ereignis den Wert der Zeitmarke, sodass jedes Ereignis in der Folge zu einem anderen Zeitpunkt eintrifft.
- **Position**: Im Portlet werden für die Längen- und Breitengrade der einzelnen Ereignisse Werte innerhalb eines Bereichs willkürlich ausgewählt (z. B. `32.9525,-115.5527 5`). Der Radius bleibt unverändert.

Portlet "Beispiel-Publisher" anpassen

Sie haben die Möglichkeit, dieses Portlet anzupassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen

wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Zugehörige Verweise:

„Einstellungen des Beispiel-Publisher-Portlets" auf Seite 173
Anpassen des Beispiel-Publisher-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Beispielereignisse mit XML erstellen

Auf der Registerkarte **Ereignis-CAP** können Sie eine Beispielvorlage für ein CAP-Ereignis auswählen, die Sie zum Anzeigen, Ändern und Veröffentlichen von Ereignissen verwenden können.

Vorbereitende Schritte

Wählen Sie anfänglich eine Ereigniskategorie aus. Die Kategorien stellen die primären Bereiche dar, in die Ereignisse unterteilt sind.

Tabelle 33. Ereigniskategorien

Kategorie	Beschreibung
CBRNE	Chemische, biologische, radiologische, nukleare oder hochexplosive Bedrohung oder Angriff
Umweltbedingt	Verschmutzung und anderes Umweltereignis
Feuer	Brandbekämpfung und Feuerwehr
Geophysisch	Geophysisches Ereignis, einschließlich Erdrutsch
Gesundheit	Medizinisches und gesundheitswesenbezogenes Ereignis
Infrastruktur	Ereignis im Zusammenhang mit Versorgungsunternehmen, Telekommunikation oder anderer nicht transportbezogener Infrastruktur
Meteorologisch	Meteorologisches Ereignis, einschließlich Hochwasser
Rettungswesen	Rettung und Bergung
Sicherheit	Allgemeines Notfallsystem und öffentliche Sicherheit
Sicherheit/Schutz	Strafverfolgung, Militär, innere und örtliche/private Sicherheit
Transportwesen	Öffentliches und privates Transportwesen
Andere	Andere Ereignisse

Informationen zu diesem Vorgang

Weitere Informationen zu Ereigniseigenschaften erhalten Sie über den Link am Ende des Themas zum Details-Portlet.

Vorgehensweise

1. Klicken Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Demonstration Tools** > **Sample Event Publisher** (Intelligent Operations > Demonstrationstools > Beispiel-Publisher).
2. Klicken Sie auf die Registerkarte **Ereignis-CAP**.
3. Wählen Sie in der Liste **Kategorie** eine Ereigniskategorie aus.
4. Wählen Sie für das Feld **Ereignisnachricht** eine der folgenden Optionen aus:
   - Um die XML für die entsprechende vorgeschriebene CAP-Nachricht automatisch in das Feld **Ereignisnachricht** einzufügen, wählen Sie aus der Liste **Beispielereignis** ein Ereignis aus. Sie können die XML ihren Anforderungen entsprechend bearbeiten.
   - Geben Sie im Feld **Ereignisnachricht** die XML für die CAP-Nachricht ganz von Neuem manuell ein.

5. Geben Sie im Feld **Ereignisinstanzzähler** die Anzahl der erforderlichen Nachrichten ein oder verwenden Sie die Pfeile, um die Anzahl der erforderlichen Nachrichten auszuwählen. Sie können eine einzelne CAP-Nachricht oder eine automatisierte Folge von Nachrichten übergeben.
6. Optional: Wählen Sie das Kontrollkästchen **Ereignisse willkürlich auswählen** aus. Wenn Sie **Ereignisse willkürlich auswählen** auswählen, wird eine Folge von CAP-Nachrichten mit willkürlich ausgewählten IDs veröffentlicht. Die Nachrichten werden in inkrementellen Zeitintervallen und an willkürlich ausgewählten Standorten in einem Bereich ausgewählt.
7. Klicken Sie auf **Submit event** (Ereignis übergeben).

Ergebnisse

Der Beispiel-Publisher füllt das IBM Intelligent Operations Center mit Ereignissen auf und kann KPIs auslösen.

Zugehörige Konzepte:

„Details" auf Seite 287
Mit dem Portlet "Details" können Sie in IBM Intelligent Operations Center Ereignisse anzeigen, überwachen und verwalten.

Neue CAP-Ereignisse erstellen oder bestehende Ereignisse ohne XML aktualisieren

Auf der Registerkarte **Ereignisformular** können Sie ein Formular ausfüllen, um neue CAP-Ereignisse zu erstellen oder bestehende Ereignisse ohne Verwendung von XML zu aktualisieren.

Informationen zu diesem Vorgang

Sie können das Formular verwenden, um ein neues Ereignis oder ein Ereignis auf der Basis von Werten aus einem bestehenden Ereignis zu erstellen. Wenn Sie ein Ereignis auf der Basis eines bestehenden Ereignisses erstellen, können Sie die CAP-Alert-ID verwenden, um auf das bestehende Ereignis zu verweisen. Alle Werte, die Sie im Formular eingeben, überschreiben Werte, die aus dem bestehenden CAP-Ereignis übernommen wurden.Weitere Informationen zu Ereigniseigenschaften erhalten Sie über den Link am Ende des Themas zum Details-Portlet.

Vorgehensweise

1. Klicken Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Demonstration Tools** > **Sample Event Publisher** (Intelligent Operations > Demonstrationstools > Beispiel-Publisher).
2. Klicken Sie auf die Registerkarte **Ereignisformular**.
3. Um eine Quelle für das Ereignis anzugeben, klicken Sie neben "Quelle" auf eine der folgenden Optionen:
   - Um ein neues Ereignis mit Werten zu erstellen, die auf den im Formular eingegebenen Werten basieren, klicken Sie auf **Neu**.
   - Um ein Ereignis mit Werten, die auf einem bestehenden Ereignis in der CAP-Ereignistabelle basieren, bei Verwendung der CAP-Alert-ID zu erstellen, klicken Sie auf **Vorhanden**.
4. Geben Sie im Feld **ID** eine ID ein, je nachdem, ob Sie ein neues Ereignis oder ein Ereignis auf der Basis einer bestehenden CAP-Alert-ID erstellen:
   - Wenn Sie ein neues Ereignis erstellen, geben Sie optional einen Wert für **ID** ein. Wenn Sie keinen Wert eingeben, wird eine eindeutige ID für Sie erstellt.
   - Wenn Sie ein Ereignis auf der Basis einer bestehenden CAP-Alert-ID erstellen, geben Sie die CAP-Alert-ID für **ID** ein. Alle Werte, die Sie im Formular eingeben, überschreiben Werte, die aus dem bestehenden CAP-Ereignis übernommen wurden.
5. Wenn Sie ein neues Ereignis erstellen, geben Sie im Feld **Ereignistyp** einen der folgenden Ereignistypen ein:

Alert Ein neues Ereignis.

Aktualisierung
Eine Aktualisierung eines zuvor erstellten Ereignisses.

Abbruch
Ein Abbruch eines zuvor erstellten Ereignisses.

6. Geben Sie im Feld **Überschrift** eine Überschrift ein.
7. Wählen Sie in der Liste **Nachrichtentyp** einen Nachrichtentyp aus.
8. Wenn Sie ein neues Ereignis erstellen, wählen Sie in der Liste **Ereigniscode** die Option **Ereignis** oder **Vorfall** aus. Ein Vorfall hat einen höheren Stellenwert als ein Ereignis.
9. Wählen Sie in der Liste **Kategorie** eine Kategorie aus.
10. Wählen Sie in der Liste **Dringlichkeit** eine Dringlichkeit aus.
11. Wählen Sie in der Liste **Schweregrad** einen Schweregrad aus.
12. Wählen Sie in der Liste **Wahrscheinlichkeit** eine Wahrscheinlichkeit aus.
13. Geben Sie im Feld **Beschreibung** eine Beschreibung ein.
14. Geben Sie im Feld **Absender** eine Beschreibung des Absenders des Ereignisses ein.
15. Wählen Sie im Feld **Ereignisinstanzzähler** die Anzahl der erforderlichen Nachrichten aus. Sie können eine einzelne CAP-Nachricht oder eine automatisierte Folge von Nachrichten übergeben.
16. Optional: Wählen Sie das Kontrollkästchen **Ereignisse willkürlich auswählen** aus. Wenn Sie **Ereignisse willkürlich auswählen** auswählen, wird eine Folge von CAP-Nachrichten mit willkürlich ausgewählten IDs veröffentlicht. Die Nachrichten werden in inkrementellen Zeitintervallen und an willkürlich ausgewählten Standorten in einem Bereich ausgewählt.
17. Klicken Sie auf **Submit event** (Ereignis übergeben).

Zugehörige Konzepte:

„Details” auf Seite 287
Mit dem Portlet "Details" können Sie in IBM Intelligent Operations Center Ereignisse anzeigen, überwachen und verwalten.

Benachrichtigungen testen

Verwenden Sie die Registerkarte **Benachrichtigung** zum Erstellen von Testbenachrichtigungen, um das Subsystem für Benachrichtigungen im IBM Intelligent Operations Center zu testen.

Informationen zu diesem Vorgang

Füllen Sie auf der Registerkarte **Benachrichtigung** das Formular aus, um einen Alert für angegebenen Gruppen zu senden. Eine Alertbenachrichtigung im Portlet "Benachrichtigungen" wird für einen bestimmten Benutzer nur angezeigt, wenn der Benutzer ein Mitglied einer der in der Benachrichtigung angegebenen Empfangsgruppen ist.

Vorgehensweise

1. Klicken Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Demonstration Tools** > **Sample Event Publisher** (Intelligent Operations > Demonstrationstools > Beispiel-Publisher).
2. Klicken Sie auf die Registerkarte **Benachrichtigung**.
3. Wählen Sie zum Erstellen eines Alerts in der Liste **Typ** die Option `Alert` aus.
4. Optional: Wählen Sie in der Liste **Kategorie** eine Kategorie aus.
5. Optional: Geben Sie im Feld **Überschrift** eine Überschrift ein.
6. Optional: Geben Sie im Feld **Beschreibung** eine Beschreibung ein.
7. Optional: Geben Sie im Feld **Absender** eine Beschreibung des Senders des Ereignisses ein.

8. Optional: Geben Sie im Feld **Sent to Groups** (Empfangsgruppen) eine durch Strichpunkte getrennte Liste von Gruppen ein, an die der Alert gesendet werden soll, z. B. `;CityWideOperator;CityWideExecutive;`.

   Anmerkung: Zusätzlich zum Einfügen eines Strichpunkts zwischen den jeweiligen Gruppennamen müssen Sie sicherstellen, dass Sie einen Strichpunkt am Anfang der Liste und am Ende der Liste einfügen.
   Wenn diese Alertbenachrichtigung veröffentlicht wird, wird sie im Portlet "Benachrichtigungen" nur für Benutzer angezeigt, die zu den Gruppen "CityWideOperator" und "CityWideExecutive" gehören.
9. Optional: Führen Sie nach Bedarf einen der folgenden Schritte aus:
   - Geben Sie im Feld **Refers to Alerts** (Bezieht sich auf Alerts) eine durch Strichpunkte getrennte Liste mit CAP-Ereignis-IDs ein, auf die der neue Alert verweist.
   - Geben Sie im Feld **Refers to KPIs** (Bezieht sich auf KPIs) eine durch Strichpunkte getrennte Liste mit KPIs ein, auf die der neue Alert verweist.
10. Klicken Sie auf **Submit Notification** (Benachrichtigung übergeben).

Zugehörige Konzepte:

„Benachrichtigungen” auf Seite 302
Mit dem Portlet "Benachrichtigungen" können Sie Alertnachrichten sowie Details zu diesen Nachrichten anzeigen.

Erstellung von Ereignisscripts

Mit dem Portlet "Erstellung von Ereignisscripts" können Sie ein Script zum Erstellen einer sequenziellen Liste von Ereignissen schreiben, die nacheinander in vorgegebenen Zeitintervallen veröffentlicht werden sollen.

Starten Sie das Portlet "Erstellung von Ereignisscripts", indem Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Demonstration Tools** > **Event Scripting** (Intelligent Operations > Demonstrationstools > Erstellung von Ereignisscripts) klicken.

Im Portlet "Erstellung von Ereignisscripts" können Sie ein Script erstellen, das über die in der Tabelle mit Beispielereignissen in der IBM Intelligent Operations Center-Datenbank aufgeführten Ereignis-IDs auf Ereignisse verweist, die veröffentlicht werden sollen. In diesem Script können Sie angeben, in welchem zeitlichen Abstand die Ereignisse veröffentlicht werden sollen. Bei der Ausführung des Scripts werden Ereignisse über das Back-End veröffentlicht. Der Ereignisablauf ist allerdings derselbe wie für Ereignisse, die von externen Quellen in das System gelangen.

Sie können die Ereignisse auch aus dem Portlet "IBM Intelligent Operations Center-Datenbank" löschen. Wenn Sie die Ereignisse aus dem Portlet "IBM Intelligent Operations Center-Datenbank" löschen, werden alle im Portlet "Karte" und im Portlet "Details" angezeigten Ereignisse gelöscht.

Vor einer Verwendung des Portlets "Erstellung von Ereignisscripts" können Sie die Ereignisse in der Tabelle mit Beispielereignissen in der IBM Intelligent Operations Center-Datenbank anzeigen.

Erstellen Sie ein JSON-Script entsprechend dem im Portlet "Erstellung von Ereignisscripts" bereitgestellten Beispiel; mit diesem Script wird eine sequenzielle Liste von Ereignissen definiert, die in vorgegebenen Zeitintervallen veröffentlicht werden. Vor der Ausführung dieses Scripts müssen Sie es bereinigen und überprüfen, indem Sie auf **Bereinigen und prüfen** klicken.

Ereignisse mit einer bestimmten ID können nur einmal veröffentlicht werden. Sollen Ereignisse mit einer bestimmten ID erneut gesendet werden, müssen Sie zunächst alle Ereignisse aus der IBM Intelligent Operations Center-Datenbank löschen. Bei Auswahl des Kontrollkästchens **IDs willkürlich auswählen** dagegen veröffentlicht das Portlet dieselben Ereignisse erneut, weist ihnen jedoch willkürlich ausgewählte IDs zu.

Beispielereignisse und KPI-Ereignisse in der Tabelle mit Beispielereignissen anzeigen

Das Portlet "Erstellung von Ereignisscripts" veröffentlicht Beispielereignisse aus der Tabelle mit Beispielereignissen in der IBM Intelligent Operations Center-Datenbank. Verwenden Sie die folgende Prozedur, um die Ereignisse in der Tabelle mit Beispielereignissen anzuzeigen.

Vorgehensweise

1. Verwenden Sie einen VNC-Client, um sich beim Datenserver als Rootbenutzer anzumelden, und öffnen Sie anschließend ein Befehlsfenster. Geben Sie in den folgenden Schritten Befehle im Befehlsfenster ein, das Sie gerade auf dem Datenserver geöffnet haben.
2. Um DB2 Control Center öffnen zu können, müssen Sie die Zugriffssteuerung vorübergehend inaktivieren; geben Sie den folgenden Befehl ein: `xhost +`
3. Zeigen Sie im DB2 Control Center die Beispielereignisse an, die in der Tabelle mit Beispielereignissen enthalten sind, und rufen Sie die Beispielereignis-IDs ab:
   a. Geben Sie die folgenden Befehle ein, um DB2 Control Center zu öffnen:
      ```
      su - db2inst1
      db2cc
      ```
   b. Klicken Sie im DB2 Control Center auf **Alle Datenbanken** > **IOCDB** > **Tables** > **REF_SAMPLEEVENTS**.
   c. Klicken Sie mit der rechten Maustaste auf die Tabelle **REF_SAMPLEEVENTS** und anschließend auf **Öffnen**. Die Tabelle mit Beispielereignissen enthält 40 Zeilen, jedoch werden nach Veröffentlichung der Ereignisse nur die Ereignisse 1-8 im Portlet "Details" angezeigt. Mit den anderen Ereignissen werden KPIs getestet. Wenn Sie das Kontrollkästchen **IDs willkürlich auswählen** im Portlet "Erstellung von Ereignisscripts" auswählen, können Sie dieselben acht Ereignisse wiederholt veröffentlichen.
   d. Vermerken Sie für jedes Beispielereignis die **SAMPLEID**, auf die zu verweisen ist, wenn Sie Ereignisscripts im Portlet "Erstellung von Ereignisscripts" erstellen. Der Wert von **SAMPLEID** entspricht der Ereignis-ID.
4. Wenn Sie mit der Anzeige der Beispielereignisse fertig sind, schließen Sie DB2 Control Center.
5. Um zurück zum Rootbenutzer zu wechseln, geben Sie den folgenden Befehl ein: `exit`
6. Um die Zugriffssteuerung erneut zu aktivieren, geben Sie den folgenden Befehl ein: `xhost -`

Zugehörige Konzepte:

„Beispiel-KPIs" auf Seite 129
Im Rahmen des IBM Intelligent Operations Center werden auch Beispiel-KPIs zur Verfügung gestellt. Die Beispiel-KPIs dienen als Anhaltspunkt und sollen Sie bei der Implementierung verschiedener KPI-Typen mit dem IBM WebSphere Business Monitor Development Toolkit unterstützen. Es werden Beispielüberwachungsmodelle aus dem Bereich Wasser, Transport und öffentliche Sicherheit bereitgestellt.

Ereignisscript erstellen

Erstellen Sie ein Ereignisscript, das eine Folge von Ereignissen in vordefinierten Zeitintervallen veröffentlicht.

Vorbereitende Schritte

Bevor Sie das Portlet "Erstellung von Ereignisscripts" zur Veröffentlichung von Ereignissen verwenden, können Sie die Ereignisse in der Tabelle mit Beispielereignissen in der IBM Intelligent Operations Center-Datenbank anzeigen.

Informationen zu diesem Vorgang

Führen Sie folgende Schritte aus, um ein Ereignisscript im Portlet "Erstellung von Ereignisscripts" zu erstellen.

Anmerkung: Ereignisse mit einer bestimmten ID können nur einmal veröffentlicht werden. Um ein Ereignis mit derselben ID wiederholt veröffentlichen zu können, klicken Sie auf **Datenbank zurücksetzen**, um alle Ereignisse aus der IBM Intelligent Operations Center-Datenbank zu löschen. Um alternativ dazu dieselben Ereignisse erneut mit willkürlich ausgewählten IDs zu veröffentlichen, aktivieren Sie das Kontrollkästchen **IDs willkürlich auswählen**.

Vorgehensweise

1. Klicken Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Demonstration Tools** > **Event Scripting** (Intelligent Operations > Demonstrationstools > Erstellung von Ereignisscripts) .
2. Verwenden Sie das im Portlet "Erstellung von Ereignisscripts" bereitgestellte Beispiel, um ein JSON-Script zu erstellen; mit diesem Script wird eine sequenzielle Liste von Ereignissen definiert, die in vordefinierten Zeitintervallen veröffentlicht werden; geben Sie das Script im Feld auf der linken Seite des Beispiels ein. Das im Portlet "Erstellung von Ereignisscripts" bereitgestellte JSON-Beispielscript wird auch im folgenden Code angezeigt:

```
[
    {
        "id": 2
        //ID of element in Sample Events table
        "delayAfter": 4000
        //Milliseconds to wait after publishing the event with the current ID
    },
    {}, //Empty objects are ignored
    {
        "id": 1
        //If the command specifies only an ID, the next command is processed
        //directly after the previous command
    },
    {
        "delayAfter": 0
        //If the command specifies only a delay, no event is published and the
        //script waits until the next command is due
    }
]
```

3. Optional: Um dieselben Ereignisse erneut mit willkürlich ausgewählten IDs zu veröffentlichen, aktivieren Sie das Kontrollkästchen **IDs willkürlich auswählen**.
4. Erforderlich: Um das Script vor der Ausführung zu bereinigen und zu überprüfen, klicken Sie auf **Bereinigen und prüfen**. Die Syntax des Scripts wird geprüft und Kommentare werden entfernt. Wenn eine falsche Markup im Script erkannt wird, die nicht aufgelöst werden kann, wird eine Nachricht angezeigt.
5. Klicken Sie auf **Ereignisscript ausführen**, um das Script auszuführen.
6. Um alle Ereignisse aus dem IBM Intelligent Operations Center-Datenbank zu entfernen und zu verhindern, dass das Script weitere Ereignisse veröffentlicht, klicken Sie auf **Datenbank zurücksetzen**.

Zugehörige Tasks:

„Beispielereignisse und KPI-Ereignisse in der Tabelle mit Beispielereignissen anzeigen" auf Seite 115
Das Portlet "Erstellung von Ereignisscripts" veröffentlicht Beispielereignisse aus der Tabelle mit Beispielereignissen in der IBM Intelligent Operations Center-Datenbank. Verwenden Sie die folgende Prozedur, um die Ereignisse in der Tabelle mit Beispielereignissen anzuzeigen.

KPIs erstellen und integrieren

KPI-Modelle (Key Performance Indicator) können mit einem Entwicklungstoolkit zur Geschäftsüberwachung und einem KPI-Managementportlet erstellt und geändert werden.

Das IBM WebSphere Business Monitor-Entwicklungstoolkit kann mit Rational Application Developer installiert werden. Beides ist im Lieferumfang von IBM Intelligent Operations Center enthalten. Das IBM WebSphere Business Monitor-Entwicklungstoolkit kann auch mit WebSphere Integration Developer installiert werden.

Bevor Sie einen KPI definieren oder ändern, müssen Sie den Common Alerting Protocol-Alert (CAP-Alert) kennen, auf dem der KPI basiert. Beispiel: Wenn Sie einen KPI definieren, um den Stand einer Wasserquelle zu verfolgen, müssen Sie die CAP-Elemente kennen, die die zu verfolgenden Elemente enthalten, wie z. B. den Namen der Wasserquelle und die Wassertiefe in Metern.Nachdem ein KPI auf diese Weise hinzugefügt oder geändert wurde, muss er auf dem IBM WebSphere Business Monitor-Server implementiert werden.

Weitere Informationen zur Verwendung von IBM WebSphere Business Monitor und des IBM WebSphere Business Monitor-Entwicklungstoolkits finden Sie im Information Center für IBM WebSphere Business Monitor.

Wenn Sie KPI-Modelle und Messwerte über IBM WebSphere Business Monitor erstellt haben, können Sie das Portlet "Key Performance Indicators (KPIs)" verwenden, um KPIs zu entwickeln und zu ändern.

Zugehörige Konzepte:

„Beispiel-KPIs” auf Seite 129
Im Rahmen des IBM Intelligent Operations Center werden auch Beispiel-KPIs zur Verfügung gestellt. Die Beispiel-KPIs dienen als Anhaltspunkt und sollen Sie bei der Implementierung verschiedener KPI-Typen mit dem IBM WebSphere Business Monitor Development Toolkit unterstützen. Es werden Beispielüberwachungsmodelle aus dem Bereich Wasser, Transport und öffentliche Sicherheit bereitgestellt.

„Ereignisse und KPIs” auf Seite 97
Das IBM Intelligent Operations Center verarbeitet Ereignisse und KPIs (Key Performance Indicators), um zu bestimmen, wie Informationen angezeigt werden.

„KPIs anpassen” auf Seite 177
Im IBM Intelligent Operations Center können Sie KPI-Modelle (Key Performance Indicator-Modelle) an Ihre Geschäftsprozesse anpassen.

Zugehörige Verweise:

„Mit der Lösung bereitgestellte Tools installieren” auf Seite 70
Im Lieferumfang von IBM Intelligent Operations Center sind Toolkits und Entwicklungstools enthalten. Diese werden bei der Anpassung von IBM Intelligent Operations Center verwendet.

Zugehörige Informationen:

Information Center für IBM WebSphere Business Process Management Version 7.0

Monitormodelle und KPIs

Ein Monitormodell definiert Messwerte und KPIs (Key Performance Indicators), ihre Abhängigkeiten von eingehenden Ereignissen, Bedingungen, die Geschäftsaktionen erfordern, und abgehende Ereignisse, die die Bedingungen melden, die möglicherweise Geschäftsaktionen auslösen.

Ein Monitormodell kann die folgenden Untermodelle enthalten:

- Monitordetailmodell
- KPI-Modell
- Dimensionsmodell
- Visuelles Modell
- Ereignismodell

Das Monitordetailmodell enthält einen Großteil der Monitormodellinformationen.

Die vom IBM Intelligent Operations Center bereitgestellten Beispielmonitormodelle verwenden keine visuellen Modelle oder Dimensionsmodelle.

Das Monitordetailmodell definiert einen oder mehrere Monitoring-Kontexte. Ein Monitoring-Kontext definiert die Informationen, die aus einem oder mehreren eingehenden Ereignissen erfasst und überwacht werden sollen. Für das IBM Intelligent Operations Center sind überwachte Entitäten CAP-Alerts. Die aus diesen Alerts erfassten Informationen werden zum Berechnen eines KPI verwendet.

Das KPI-Modell enthält einen oder mehrere KPI-Kontexte. Diese definieren die KPIs und die zugehörigen Trigger und Ereignisse. KPI-Kontexte können eingehende Ereignisse verarbeiten, wiederkehrende Wartezeittrigger auswerten und abgehende Ereignisse senden. Beispiel: Der Kontext kann prüfen, ob sich ein KPI außerhalb des gültigen Bereichs befindet, und eine Benachrichtigung senden.

Das Ereignismodell bezieht sich auf alle eingehenden und abgehenden Ereignisdefinitionen, die im Monitormodell verwendet werden. Es verweist auf Schemas, die die Struktur einzelner Ereignisteile beschreiben.

Zugehörige Konzepte:

„Beispiel-KPIs" auf Seite 129
Im Rahmen des IBM Intelligent Operations Center werden auch Beispiel-KPIs zur Verfügung gestellt. Die Beispiel-KPIs dienen als Anhaltspunkt und sollen Sie bei der Implementierung verschiedener KPI-Typen mit dem IBM WebSphere Business Monitor Development Toolkit unterstützen. Es werden Beispielüberwachungsmodelle aus dem Bereich Wasser, Transport und öffentliche Sicherheit bereitgestellt.

Zugehörige Informationen:

Information Center für IBM Business Monitor

Monitoring-Kontextinstanzen

Eine Monitoring-Kontextinstanz enthält Informationen, die zu einem bestimmten Zeitpunkt in einem Monitoring-Kontext erfasst werden.

Für das IBM Intelligent Operations Center entspricht eine Monitoring-Kontextinstanz einem CAP-Alert. Wenn ein CAP-Alert empfangen wird, wird eine Monitoring-Kontextinstanz erstellt oder wiederverwendet und die Messwerte in dieser Kontextinstanz werden mit den CAP-Alertwerten anhand des Monitoring-Kontexts aufgefüllt.

Ein Monitoring-Kontext kann definiert werden, um eine neue Instanz für jeden CAP-Alert zu erstellen oder um eine bestehende Instanz wiederzuverwenden. Beispiel: Wenn ein KPI den durchschnittlichen wöchentlichen Wasserstand für eine bestimmte Ressource berechnen soll, deren Wasserstand täglich geprüft wird, würden Sie eine neue Überwachungskontextinstanz für jeden CAP-Alert erstellen. Jede Instanz würde einen täglichen Wasserstand enthalten und der KPI würde einen Mittelwert aus den Messwerten, die in einem Zeitraum von sieben Tagen ermittelt wurden, berechnen.

KPIs werden mit den Messwerten berechnet, die für einen Monitoring-Kontext definiert wurden. Wenn Sie einen Aggregations-KPI definieren, geben Sie den Monitoring-Kontext und die Metrik an, die als Eingabe für die KPI-Aggregationsfunktion verwendet wird. Wenn der KPI ausgewertet wird, werden die Messwerte für die Monitoring-Kontextinstanzen von der Aggregationsfunktion zur Berechnung des KPI-Werts verwendet.

Zugehörige Konzepte:

„Beispiel-KPIs" auf Seite 129
Im Rahmen des IBM Intelligent Operations Center werden auch Beispiel-KPIs zur Verfügung gestellt. Die Beispiel-KPIs dienen als Anhaltspunkt und sollen Sie bei der Implementierung verschiedener KPI-Typen mit dem IBM WebSphere Business Monitor Development Toolkit unterstützen. Es werden Beispielüberwachungsmodelle aus dem Bereich Wasser, Transport und öffentliche Sicherheit bereitgestellt.

Zugehörige Informationen:


Information Center für IBM Business Monitor

KPIs modellieren

Modellieren Sie KPIs mit Rational Application Developer oder WebSphere Integration Developer mit dem IBM WebSphere Business Monitor-Entwicklungstoolkit. Rational Application Developer und das IBM WebSphere Business Monitor-Entwicklungstoolkit sind im Lieferumfang von IBM Intelligent Operations Center enthalten.

Informationen zu diesem Vorgang

KPIs werden mit Rational Application Developer oder WebSphere Integration Developer mit dem IBM WebSphere Business Monitor-Entwicklungstoolkit modelliert. Weitere Informationen zur Verwendung dieser Tools finden Sie im jeweiligen Information Center für diese Produkte.

Monitormodelle sind in Geschäftsüberwachungsprojekten enthalten. Modelle und Projekte werden mit den Geschäftsüberwachungsassistenten von Rational Application Developer erstellt, die vom IBM WebSphere Business Monitor-Entwicklungstoolkit bereitgestellt werden.

Gehen Sie wie folgt vor, um einen KPI zu modellieren.

Vorgehensweise

1. Machen Sie sich mit dem CAP-Alert vertraut, der vom IBM Intelligent Operations Center empfangen wird.
2. Machen Sie sich mit dem Zweck des KPI vertraut. Generiert der KPI eine Aktion, wenn ein Grenzwert erreicht oder überschritten wird? Wird der KPI verwendet, um historische oder statistische Daten zu berechnen?
3. Bestimmen Sie den Namen für den Monitoring-Kontext. Die Namenskonvention von IBM Intelligent Operations Center verwendet den CAP-Ereignistyp als Namen. Die von IBM Intelligent Operations Center bereitgestellten Beispiele erstellen separaten Monitoring-Kontext für jede CAP-Alertnachricht, die an den IBM WebSphere Business Monitor gesendet wird.
4. Definieren Sie im Rational Application Developer oder WebSphere Integration Developer mit dem IBM WebSphere Business Monitor-Entwicklungstoolkit das eingehende Ereignis, den Schlüssel und die Gruppe von Messwerten für den Überwachungskontext. Das eingehende Ereignis definiert die Alertnachricht, die vom Kontext überwacht wird, einen Schlüssel, der die Kontextinstanz eindeutig definiert und die Messwerte, die die Informationen definieren, die aus der CAP-Alertnachricht extrahiert werden.
5. Geben Sie das CAP-Schema für das Ereignis an. Das Schema muss im Überwachungsprojekt enthalten sein. Das IBM Intelligent Operations Center stellt eine Kopie des CAP-Schemas V1.2 im Beispielmodellierungsprojekt `icoc_sample_monitor_models` bereit.
6. Geben Sie den Namen und die ID für jedes eingehende Geschäftsüberwachungsereignis an. Ereignis-IDs dürfen keine Leerzeichen oder Sonderzeichen enthalten. Standardmäßig wird die ID aus dem Namen mit Unterstrichen als Ersatz für Leerzeichen erstellt. Alle Beispiele, die vom IBM Intelligent Operations Center bereitgestellt werden, verwenden Standardelement-IDs.
7. Geben Sie das Schema an. Das Schema definiert die Struktur des eingehenden Ereignisses für den IBM WebSphere Business Monitor.

8. Definieren Sie beliebige Filter für CAP-Nachrichten. Beschränken Sie z. B. die Überwachung auf bestimmte Ereignistypen oder auf den Schweregrad.
9. Geben Sie die Messwerte an, die aus der CAP-Nachricht extrahiert werden sollen.
10. Definieren Sie einen Kontextschlüssel, der die Monitoring-Kontextinstanz eindeutig bestimmt. Schlüsselwerte werden vom eingehenden Ereignis angegeben, wenn der Monitoring-Kontext erstellt wird.
11. Geben Sie an, ob eingehende Ereignisse korrelieren sollen.
12. Geben Sie den KPI-Kontext an. Ein KPI-Kontext ist ein Container für KPIs und die zugehörigen Trigger und Ereignisse. Im Gegensatz zu einem Monitoring-Kontext enthält ein KPI-Kontext keine Schlüssel oder Messwerte. Ein KPI-Kontext muss als Container vor der Erstellung von KPIs erstellt werden.
13. Erstellen Sie den KPI im zuvor definierten KPI-Kontext.
14. Geben Sie den KPI-Typ an: **Dezimal** oder **Dauer**.
15. Definieren Sie die KPI-Bereiche, Werte und Farbanzeiger. Die meisten Beispiel-KPIs von IBM Intelligent Operations Center definieren drei Bereiche und zugehörige Farben.

Tabelle 34. Bereichs- und Farbdefinitionen für Beispiel-KPI

Name	Farbe	RGB
Akzeptabel	grün	699037
Vorsicht	gelb	FDBA1A
Take action (Maßnahme ergreifen)	rot	C32E14

16. Definieren Sie, wie der KPI-Wert berechnet wird. KPI-Werte werden mit einer von zwei Methoden bestimmt. Wenn der Wert aus Messwerten mit einer Aggregationsfunktion stammt, wird der KPI als Aggregations-KPI bezeichnet. Wenn der Wert auf der Basis anderer KPIs oder benutzerdefinierter XPath-Funktionen berechnet wird, wird der KPI als Ausdrucks-KPI bezeichnet.

    In den IBM Intelligent Operations Center-Beispielen werden die KPIs der niedrigsten Ebene (die KPIs ohne untergeordnete Elemente) als Aggregations-KPIs definiert. KPIs der höheren Ebene (KPIs mit untergeordneten Elementen) werden als Ausdrucks-KPIs definiert.

    Werte für Aggregations-KPIs werden aus Messwerten berechnet, die mit in CAP-Alertnachrichten gesendeten Daten aufgefüllt werden, die an den IBM WebSphere Business Monitor-Server gesendet werden. Anschließend wird eine Aggregationsfunktion für diese Daten ausgeführt. Zu den Aggregationsfunktionen gehören folgende:

    - `average`
    - `maximum`
    - `minimum`
    - `sum`
    - `number of occurrences`
    - `standard deviation`

    Die Werte werden als quantifizierbare Messwerte ausgedrückt. Beispiel: Durchschnittliche Reaktionszeit auf Verbrechen (5 Minuten, 7 Sekunden) oder durchschnittlicher Wasserstand (100.5).

    Werte für Ausdrucks-KPIs werden aus KPI-Bereichen und -Berechnungen berechnet. In den IBM Intelligent Operations Center-Beispielen verfügen die übergeordneten KPIs über Berechnungen, die dazu führen, dass der KPI abhängig von den Werten der untergeordneten KPIs den Wert 0, 1 oder 2 annimmt. Der Wert 0 ist dem Bereich "Akzeptabel" zugeordnet, 1 dem Bereich "Vorsicht" und 2 dem Bereich "Maßnahme ergreifen". Die Beispiele verwenden Berechnungsausdrücke, um den KPI-Wert auf die höchste Dringlichkeit der zugehörigen untergeordneten Elemente zu setzen.
17. Optional: Legen Sie für einen Aggregations-KPI den Zeitfilter an. Aggregation-KPIs können über optionale Zeitfilter verfügen, die den Zeitraum beschränken, in dem der KPI-Wert berechnet wird. Das Zeitintervall kann ein Wiederholungsintervall (z. B. die letzte abgeschlossene oder die laufende Peri-

ode), ein gleitendes Intervall oder ein festes Intervall sein. Alle Beispiel-Aggregations-KPIs von IBM Intelligent Operations Center besitzen definierte Zeitfilter.

18. Optional: Geben Sie einen Datenfilter für den KPI an. Beispiel: Wenn die durchschnittliche Reaktionszeit auf Verbrechen für Bezirk 1 und keine anderen Bereiche berechnet werden soll, kann ein Datenfilter verwendet werden, um alle anderen Monitoring-Kontexte zu entfernen .
19. Definieren Sie, wie KPI-Werte aktualisiert werden, einschließlich Trigger, eingehender Ereignisse für den IBM WebSphere Business Monitor-Server und abgehender Ereignisse für das IBM Intelligent Operations Center.
20. Testen Sie den KPI. Das Entwicklungstoolkit von IBM WebSphere Business Monitor enthält eine Testumgebung zum Testen der KPIs vor der Implementierung. Weitere Informationen dazu finden Sie über den Link am Ende des Themas.
21. Implementieren Sie die Monitormodellanwendung.

Zugehörige Konzepte:

„KPI-Hierarchien definieren"
Sie können Beziehungen zwischen übergeordneten und untergeordneten Elementen zwischen KPIs definieren und die Anzeige von KPIs im IBM Intelligent Operations Center gestalten. Entwerfen Sie Ihre eigenen KPI-Hierarchien, sodass Sie KPIs in einer für Ihren Geschäftsprozess geeigneten Art und Weise suchen können.

„Beispiel-KPIs" auf Seite 129
Im Rahmen des IBM Intelligent Operations Center werden auch Beispiel-KPIs zur Verfügung gestellt. Die Beispiel-KPIs dienen als Anhaltspunkt und sollen Sie bei der Implementierung verschiedener KPI-Typen mit dem IBM WebSphere Business Monitor Development Toolkit unterstützen. Es werden Beispielüberwachungsmodelle aus dem Bereich Wasser, Transport und öffentliche Sicherheit bereitgestellt.

„KPI-Ereigniskommunikation zwischen IBM WebSphere Business Monitor und IBM Intelligent Operations Center" auf Seite 123
IBM WebSphere Business Monitor kann abgehende Ereignisse von einem Monitoring- oder KPI-Kontext an IBM Intelligent Operations Center senden.

Zugehörige Tasks:

„Monitormodelle implementieren" auf Seite 126
Nach der Definition der KPIs (Key Performance Indicators) und der zugehörigen Monitormodelle müssen die Monitormodelle für den IBM WebSphere Business Monitor implementiert werden, der auf dem Anwendungsserver von IBM Intelligent Operations Center ausgeführt wird.

Zugehörige Verweise:

„Mit der Lösung bereitgestellte Tools installieren" auf Seite 70
Im Lieferumfang von IBM Intelligent Operations Center sind Toolkits und Entwicklungstools enthalten. Diese werden bei der Anpassung von IBM Intelligent Operations Center verwendet.

Zugehörige Informationen:

Information Center für Rational Application Developer

Information Center für IBM Business Monitor

XML Path Language (XPath) 2.0 (Zweite Edition)

KPI-Hierarchien definieren

Sie können Beziehungen zwischen übergeordneten und untergeordneten Elementen zwischen KPIs definieren und die Anzeige von KPIs im IBM Intelligent Operations Center gestalten. Entwerfen Sie Ihre eigenen KPI-Hierarchien, sodass Sie KPIs in einer für Ihren Geschäftsprozess geeigneten Art und Weise suchen können.

Während IBM WebSphere Business Monitor einen KPI zulässt, der auf dem Wert eines anderen KPI basiert, ist die Definition einer Beziehung zwischen übergeordnetem und untergeordnetem Element zwi-

schen KPIs nicht erlaubt. Um diese Task zu vereinfachen, stellt das IBM Intelligent Operations Center ein Key Performance Indicators (KPIs)-Portlet für den Administrator bereit. Weitere Informationen zu diesem Portlet erhalten Sie über den Link am Ende dieses Themas.

Die Beispiel-KPIs von IBM Intelligent Operations Center definieren eine Reihe von Polizeidienststellen-KPIs mit einem hierarchischen Design wie folgt:

```
Police Department  ---------------------------- level 1
   Crime Response Time ------------------------- level 2
      Crime Response Time Precinct One ----- level 3
      Crime Response Time Precinct Two ----- level 3
```

In diesem Fall verfügt `Police Department` über ein untergeordnetes Element: `Crime Response Time`. `Crime Response Time` verfügt über zwei untergeordnete Elemente: `Crime Response Time Precinct One` und `Crime Response Time Precinct Two`.

Die zwei KPIs der Ebene 3 sind im KPI-Modell als Aggregations-KPIs definiert. Das heißt, ihre Werte werden mit einem Messwert und einer Aggregationsfunktion berechnet. Alle anderen KPIs in dieser Gruppe sind Ausdrucks-KPIs, deren Werte aus Werten der anderen KPIs berechnet werden. Beispiel:

- `Crime Response Time` basiert auf den Werten von `Crime Response Time Precinct One` und `Crime Response Time Precinct Two`.
- `Police Department` basiert auf dem Wert von `Crime Response Time`.

Das IBM Intelligent Operations Center unterstützt eine Alternative zur Verwendung des Key Performance Indicators (KPIs)-Portlets zum Definieren von KPI-Beziehungen. Das Key Performance Indicators (KPIs)-Portlet ist die Standardmethode, wobei der Parameter **`UseDBModelReader`** in der Tabelle mit Systemeigenschaften auf "true" gesetzt ist. Informationen zum Ändern der Einstellung in der Tabelle mit Systemeigenschaften erhalten Sie über den Link am Ende dieses Themas. Informationen zum Alternativverfahren für das Definieren von KPI-Beziehungen erhalten Sie über den Link am Ende dieses Themas.

Zugehörige Konzepte:

„Key Performance Indicators (KPIs)" auf Seite 178
Mit dem Portlet "Key Performance Indicators (KPIs)" können Sie KPIs (Key Performance Indicator) und ihre hierarchische Anzeige in IBM Intelligent Operations Center anpassen.

„Systemweite Konfigurationsdaten angeben" auf Seite 188
In der Tabelle mit den Systemeigenschaften von IBM Intelligent Operations Center sind IBM Intelligent Operations Center-Konfigurationsdaten gespeichert.

„KPI-Hierarchien mit OWL definieren"
Das IBM Intelligent Operations Center unterstützt die Verwendung von OWL (Web Ontology Language) als Alternative zur Verwendung des Portlets "Key Performance Indicators (KPIs)" zum Definieren von KPI-Beziehungen zwischen übergeordnetem und untergeordnetem Element.

KPI-Hierarchien mit OWL definieren

Das IBM Intelligent Operations Center unterstützt die Verwendung von OWL (Web Ontology Language) als Alternative zur Verwendung des Portlets "Key Performance Indicators (KPIs)" zum Definieren von KPI-Beziehungen zwischen übergeordnetem und untergeordnetem Element.

KPI-Beziehungen zwischen übergeordnetem und untergeordnetem Element können in OWL, die vom IBM Intelligent Operations Center gelesen und verarbeitet wird, definiert werden. Die Definitionen werden in einer RDF-Datei (Resource Description Framework) gespeichert.

Sie können angeben, ob das KPI-Datenbankmodell aus einer RDF-Datei gelesen werden soll oder nicht. Weitere Informationen zum Ändern dieser Eigenschaft in der Tabelle mit Systemeigenschaften erhalten Sie über den Link am Ende dieses Themas.

Ein Beispiel der OWL-Definitionen für die KPI-Beispielgruppe `Police Department` lautet wie folgt:

```
<icop:KPIDefinition rdf:ID="Police_Department">
<icop:KPIBase.name>Police Department</icop:KPIBase.name>
<icop:KPIBase.id>Police_Department</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_ModelDefinition
      rdf:resource= "#icoc_sample_public_safety_monitor_model"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time">
<icop:KPIBase.name>Crime Response Time</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Police_Department"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_One">
<icop:KPIBase.name>Crime Response Time Precinct One</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_One</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_Two">
<icop:KPIBase.name>Crime Response Time Precinct Two</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_Two</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >
```

Anmerkung: OWL ist eine Sprache, die auf RDF aufbaut. OWL und RDF sind ähnliche Sprachen, OWL ist jedoch stärker. OWL bietet ein umfangreicheres Vokabular, eine stärkere Syntax und kann von Maschinen besser interpretiert werden als RDF.

Zugehörige Konzepte:

„KPI-Hierarchien definieren" auf Seite 121
Sie können Beziehungen zwischen übergeordneten und untergeordneten Elementen zwischen KPIs definieren und die Anzeige von KPIs im IBM Intelligent Operations Center gestalten. Entwerfen Sie Ihre eigenen KPI-Hierarchien, sodass Sie KPIs in einer für Ihren Geschäftsprozess geeigneten Art und Weise suchen können.

„Key Performance Indicators (KPIs)" auf Seite 178
Mit dem Portlet "Key Performance Indicators (KPIs)" können Sie KPIs (Key Performance Indicator) und ihre hierarchische Anzeige in IBM Intelligent Operations Center anpassen.

„Systemweite Konfigurationsdaten angeben" auf Seite 188
In der Tabelle mit den Systemeigenschaften von IBM Intelligent Operations Center sind IBM Intelligent Operations Center-Konfigurationsdaten gespeichert.

KPI-Ereigniskommunikation zwischen IBM WebSphere Business Monitor und IBM Intelligent Operations Center

IBM WebSphere Business Monitor kann abgehende Ereignisse von einem Monitoring- oder KPI-Kontext an IBM Intelligent Operations Center senden.

Abgehende Ereignisse vom IBM WebSphere Business Monitor-Server werden in eine externe Nachrichtenwarteschlange gestellt. Das IBM Intelligent Operations Center verwendet diesen Mechanismus, um KPI-Aktualisierungen asynchron zu empfangen.

Anmerkung: Sie können angeben, ob die Verbindung zum IBM WebSphere Business Monitor SSL für eine sichere Verbindung verwenden soll. Weitere Informationen zum Ändern dieser Eigenschaft in der Systemeigenschaftentabelle erhalten Sie über den Link am Ende dieses Themas.

Zugehörige Konzepte:

„Systemweite Konfigurationsdaten angeben" auf Seite 188
In der Tabelle mit den Systemeigenschaften von IBM Intelligent Operations Center sind IBM Intelligent Operations Center-Konfigurationsdaten gespeichert.

„Die Warteschlange für eingehende Ereignisse für das IBM Intelligent Operations Center verwenden" auf Seite 106
CAP-Ereignisse können im IBM Intelligent Operations Center veröffentlicht werden, indem sie an die eingeschlossene WebSphere Message Broker-Instanz übertragen werden.

Trigger

Ein Trigger ist ein Mechanismus, der einen Vorfall erkennt und zusätzliche Verarbeitungen als Reaktion auf diesen Vorfall auslösen kann.

Die im IBM Intelligent Operations Center bereitgestellten KPI-Beispiele definieren zwei Typen von Triggern. Der erste Trigger wird ausgelöst, wenn eine CAP-Alertnachricht, die auch als eingehendes Ereignis bezeichnet wird, vom IBM WebSphere Business Monitor-Server für eine definierte KPI-Gruppe empfangen wird. Die CAP-Alertnachricht kann den KPI ändern oder auch nicht. Das IBM Intelligent Operations Center bestimmt, ob der KPI geändert wird, wenn es die Ereignisbenachrichtigung vom IBM WebSphere Business Monitor-Server empfängt.

Für abgehende Ereignisse bestimmt ein Trigger, wann das Ereignis gesendet wird.

Auf einem Ereignis basierende Trigger können verwendet werden, um Benachrichtigungen an das IBM Intelligent Operations Center zu senden, wenn sich die Eingabe für eine KPI-Berechnung ändert. Ereignistrigger können jedoch nicht verwendet werden, wenn sich ein KPI-Wert nach Ablauf eines definierten Zeitraums ändert. In den IBM Intelligent Operations Center-Beispielen werden zeitbasierte Trigger verwendet, um Benachrichtigungen an das IBM Intelligent Operations Center für diese KPIs zu senden, für die ein kurzer Zeitraum definiert ist.

Beispiel: Für `Severe Traffic Accidents KPI` ist ein stündlicher Ablauf definiert. Wenn der KPI um 10 Uhr den Wert 3 hat und keine CAP-Alertnachrichten für diesen KPI während der nächsten Stunde empfangen werden, läuft der Zeitraum ab und der KPI-Wert wird auf 0 zurückgesetzt.

Eingehende Ereignisse für IBM WebSphere Business Monitor definieren

In den IBM Intelligent Operations Center-Beispielen werden eingehende Ereignisse verwendet, um zu bestimmen, wann ein Trigger ausgelöst wird. Eingehende Ereignisse für einen KPI-Kontext werden in einer ähnlichen Art und Weise definiert wie die für einen Monitoring-Kontext.

Informationen zu diesem Vorgang

Eingehende Ereignisse werden mit Rational Application Developer oder WebSphere Integration Developer mit dem IBM WebSphere Business Monitor-Entwicklungstoolkit definiert. Weitere Informationen zur Verwendung dieser Tools finden Sie im jeweiligen Information Center für diese Produkte.

Gehen Sie wie folgt vor, um ein eingehendes Ereignis zu definieren.

Vorgehensweise

1. Wählen Sie den KPI-Kontext für das eingehende Ereignis aus.
2. Erstellen Sie das eingehende Ereignis und geben Sie den Ereignisnamen und die ID an.
3. Geben Sie das CAP-Schema an.
4. Geben Sie die Filterbedingung an.
5. Wählen Sie den KPI-Kontext aus und erstellen Sie ein neues eingehendes Ereignis.
6. Erstellen Sie einen neuen Trigger für das eingehende Ereignis.

7. Stellen Sie sicher, dass der Trigger wiederholt anwendbar ist, sodass der Trigger jedes Mal ausgelöst wird, wenn die Triggerquelle aktualisiert wird und die Triggerbedingung erfüllt wird.
8. Wählen Sie die Triggerquelle aus.
9. Definieren Sie die Triggerbedingung. Wenn die Triggerbedingung erfüllt wird, wird der Trigger ausgelöst.

Beispiel

Die Beispielmonitormodelle von IBM Intelligent Operations Center sind so definiert, dass ein Trigger jedes Mal ausgelöst wird, wenn eine CAP-Alertnachricht vom IBM WebSphere Business Monitor-Server empfangen wird.

Zugehörige Tasks:

„KPIs modellieren" auf Seite 119
Modellieren Sie KPIs mit Rational Application Developer oder WebSphere Integration Developer mit dem IBM WebSphere Business Monitor-Entwicklungstoolkit. Rational Application Developer und das IBM WebSphere Business Monitor-Entwicklungstoolkit sind im Lieferumfang von IBM Intelligent Operations Center enthalten.

Zugehörige Informationen:

Information Center für IBM Business Monitor

Information Center für Rational Application Developer

Abgehende Ereignisse für das IBM Intelligent Operations Center definieren

Abgehende Ereignisse definieren die Informationen, die vom IBM WebSphere Business Monitor an das IBM Intelligent Operations Center gesendet werden, wenn ein Trigger ausgelöst wird.

Informationen zu diesem Vorgang

Das IBM Intelligent Operations Center verwendet abgehende Benachrichtigungen, die vom IBM WebSphere Business Monitor-Server gesendet werden, um zu bestimmen, ob sich der KPI geändert hat. Wenn sich der KPI geändert hat, fragt das IBM Intelligent Operations Center die KPI-Daten vom IBM WebSphere Business Monitor-Server ab, aktualisiert die KPI-Cachedaten und aktualisiert die IBM Intelligent Operations Center-Daten.

Ausgehende Ereignisse werden mit Rational Application Developer oder WebSphere Integration Developer mit dem IBM WebSphere Business Monitor-Entwicklungstoolkit definiert. Weitere Informationen zur Verwendung dieser Tools finden Sie im jeweiligen Information Center für diese Produkte.

Gehen Sie wie folgt vor, um ein abgehendes Ereignis zu definieren.

Vorgehensweise

1. Wählen Sie den KPI-Kontext für das abgehende Ereignis aus.
2. Erstellen Sie das abgehende Ereignis und geben Sie den Ereignisnamen und die ID an.
3. Geben Sie das Benachrichtigungsschema an. Das Schema befindet sich in der Datei `ioc-notification-v1.0.xsd`. Das Schema befindet sich im Projekt `icoc_sample_monitor-models`.
4. Definieren Sie den Inhalt des abgehenden Ereignisses. Der Inhalt basiert auf dem Benachrichtigungsschema.
5. Geben Sie unter **notification** für den Wert **sentfrom** `Monitor` ein.
6. Fügen Sie dem Ereignisinhalt die Parameterelemente hinzu, wie in den folgenden Unterschritten definiert:
   a. Geben Sie für den ersten Parameter `modelID` für **parameterName** und die Monitormodell-ID für **parameterValue** an. Beispiel: `icoc_sample_public_safety_monitor_model`.

b. Fügen Sie für jeden KPI in der KPI-Gruppe Parameter hinzu, um die KPI-ID und den KPI-Wert anzugeben. Die KPI-ID wird mit dem Element **parameterName** angegeben und der KPI-Wert mit dem Element `parameterValue`. Die KPI-ID muss einem KPI in der KPI-Gruppe zugeordnet sein. Verwenden Sie die Funktion `xs:string()`, um den KPI-Wert als Zeichenfolge anzugeben. Beispiel: **parameterName** kann `Police_Department` lauten und **parameterValue** kann `xs:string(Police_Department)` lauten.

Beispiel

Im Folgenden finden Sie ein Beispiel einer Benachrichtigung, die an das IBM Intelligent Operations Center gesendet werden soll:

```
<ns1:notification>
  <ns1:notificationType> Alert</ns1:notificationType>
  <ns1:sentFrom> Monitor</ns1:sentFrom>
  <ns1:headline> Police Department KPI Changed</ns1:headline>
  <ns1:description> Police Department KPI Changed</ns1:description>
  <ns1:kpiLink> Police Department</ns1:kpiLink>
  <ns1:category> Safety</ns1:category>
  <ns1:parameter>
    <ns1:parameterName> modelId</ns1:parameterName>
  <ns1:parameterValue>
     icoc_sample_public_safety_monitor_model</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Police_Department</ns1:parameterName>
    <ns1:parameterValue> 0</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time</ns1:parameterName>
    <ns1:parameterValue> 0</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time_Precinct_One</ns1:parameterName>
    <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time_Precinct_Two</ns1:parameterName>
    <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
  </ns1:parameter>
</ns1:notification>
```

Zugehörige Tasks:

„KPIs modellieren” auf Seite 119
Modellieren Sie KPIs mit Rational Application Developer oder WebSphere Integration Developer mit dem IBM WebSphere Business Monitor-Entwicklungstoolkit. Rational Application Developer und das IBM WebSphere Business Monitor-Entwicklungstoolkit sind im Lieferumfang von IBM Intelligent Operations Center enthalten.

Zugehörige Informationen:

Information Center für IBM Business Monitor

Information Center für Rational Application Developer

Monitormodelle implementieren

Nach der Definition der KPIs (Key Performance Indicators) und der zugehörigen Monitormodelle müssen die Monitormodelle für den IBM WebSphere Business Monitor implementiert werden, der auf dem Anwendungsserver von IBM Intelligent Operations Center ausgeführt wird.

Informationen zu diesem Vorgang

Um ein Monitormodell zu implementieren, das vom IBM WebSphere Business Monitor verwendet wird, müssen Java Enterprise Edition-Projekte (JEE-Projekte) aus den definierten Modellen generiert werden. Wenn die JEE-Projekte erstellt wurden, kann die Modellanwendung als EAR-Datei exportiert werden. Die EAR-Datei kann dann im IBM WebSphere Business Monitor implementiert werden, der auf dem IBM Intelligent Operations Center Anwendungsserver ausgeführt wird.

Vorgehensweise

1. Klicken Sie in Rational Application Developer oder WebSphere Integration Developer mit dem IBM WebSphere Business Monitor-Entwicklungstoolkit auf der Registerkarte **Enterprise-Explorer** mit der rechten Maustaste auf das Monitormodell, für das eine Projektgenerierung erforderlich ist. Beispiel: `icoc_sample_public_safety_monitor_model`.
2. Klicken Sie auf **JEE-Monitorprojekte generieren**. Die folgenden Projekte werden erstellt: `modelApplication`, `modelLogic` und `modelModerator`.
3. Exportieren Sie die Monitormodellanwendung, indem Sie mit der rechten Maustaste auf das Projekt "`modelApplication`" und anschließend auf **Exportieren** > **EAR** klicken.
4. Testen Sie die KPIs vor der Implementierung der EAR-Datei in IBM WebSphere Business Monitor.
5. Implementieren Sie die EAR-Datei im IBM WebSphere Business Monitor-Server und befolgen Sie dazu die Anweisungen im Information Center für IBM WebSphere Business Monitor.

Zugehörige Informationen:

Information Center für IBM Business Monitor

Information Center für Rational Application Developer

KPI-Anzeigewerte

Die IBM Intelligent Operations Center-Ressourcenpakete können verwendet werden, um andere Anzeigewerte als die von den IBM WebSphere Business Monitor-Modellen bereitgestellten Werte verfügbar zu machen.

KPI-Anzeigenamen und Bereichsnamen werden in den IBM WebSphere Business Monitor-Beispielmodellen definiert, die mit dem IBM Intelligent Operations Center bereitgestellt werden. Zu den Beispielen für KPI-Anzeigenamen gehören folgende:

- Wasser
- Wasserqualität

Zu den Beispielen für Bereichsnamen gehören folgende:

- Statuswert "zulässig"
- Statuswert "Vorsicht"
- Statuswert "Maßnahme ergreifen"

Jedem im IBM WebSphere Business Monitor definierten Artefakt, z. B. KPI und Bereich, ist eine ID mit dem Anzeigenamen zugeordnet. IDs dürfen keine Leerzeichen enthalten, Anzeigewerte hingegen schon. Die IDs werden als Schlüssel zum Suchen von Werten in einem Ressourcenpaket verwendet. Das IBM Intelligent Operations Center verwendet diese IDs, um KPI-Anzeigewerte auszuwählen. Wenn im Ressourcenpaket keine Werte für die ID angegeben sind, werden die in der IBM WebSphere Business Monitor-Definition angegebenen Werte verwendet.

Die KPI-Anzeigewerte werden von IBM WebSphere Business Monitor mit den ISO-Sprach- und Ländercodes des IBM WebSphere Business Monitor-Servers lokalisiert. Beispiel: Der KPI-Prozentsatz mit der

Ländereinstellung `en_US` würde im Format 12.61% angezeigt werden. Mit der Ländereinstellung `fr_FR` würde er im Format 12,61% angezeigt werden. Ressourcenpaketdefinitionen werden nicht für diese Werte verwendet.

Das Ressourcenpaket mit den IBM Intelligent Operations Center-Standardeigenschaften lautet `com.ibm.iss.icoc.rest.monitor.resources.Messages.properties`. Das Paket befindet sich unter `icoc_rest_monitor_resources_utils`.

Dies ist ein Beispielressourcenpaket:

```
kpi.NO.VALUE=No data to determine the KPI value
kpi.RANGE.UNDETERMINED=undetermined
Flood_Control=Flood Control
Water_Levels=Water Levels
Flow_Discharge_City_River=Flow Discharge City River
Water_Level_City_Lake=Water Level City Lake
```

In diesem Beispiel werden die Werte von `kpi.NO.VALUE` und `kpi.RANGE.UNDETERMINED` vom IBM Intelligent Operations Center verwendet, wenn die IBM WebSphere Business Monitor-KPIs einen Nullwert zurückgeben. Beispiel: Der KPI "Water Level City Lake" ist mit einem sich wiederholenden täglichen Zeitraum definiert, der auf dem letzten vollständigen Zeitraum basiert. Wenn an einem Sonntag keine CAP-Ereignisse für diesen KPI empfangen werden und der KPI am Montag abgefragt wird, wird null zurückgegeben, da keine Daten für den vorherigen Tag verfügbar sind. Der Anzeigewert ist auf "Keine Daten zur Bestimmung des KPI-Werts" gesetzt und der Bereichsanzeigename ist auf "unbestimmt" gesetzt.

Die anderen Einträge, `Flood_Control`, `Water_Levels`, `Flow_Discharge_City_River` und `Water_Level_City_Lake`, definieren die Anzeigewerte für die KPI-IDs, die im vom IBM Intelligent Operations Center bereitgestellten Beispielmonitormodell `icoc sample water monitor model` definiert sind. Diese Einträge können alternativen Text aus den im IBM WebSphere Business Monitor-Monitor angegebenen Werten anzeigen. Beispiel: Das Ressourcenpaket kann verwendet werden, um übersetzte Werte anzuzeigen, anstatt das Modell selbst zu ändern.

Zugehörige Konzepte:

„Beispiel-KPIs” auf Seite 129
Im Rahmen des IBM Intelligent Operations Center werden auch Beispiel-KPIs zur Verfügung gestellt. Die Beispiel-KPIs dienen als Anhaltspunkt und sollen Sie bei der Implementierung verschiedener KPI-Typen mit dem IBM WebSphere Business Monitor Development Toolkit unterstützen. Es werden Beispielüberwachungsmodelle aus dem Bereich Wasser, Transport und öffentliche Sicherheit bereitgestellt.

KPIs zwischenspeichern

IBM Intelligent Operations Center-Konfigurationseinstellungen wirken sich beim Abruf von KPI-Werten aus dem IBM WebSphere Business Monitor aus.

Das IBM Intelligent Operations Center verwaltet KPI-Werte in einem Cache. Standardmäßig werden die KPIs aus IBM WebSphere Business Monitor in den Cache geladen und der Cache wird gemäß dem über die Eigenschaft **`KpiCacheRefreshInterval`** in der Systemeigenschaftentabelle angegebenen Zeitintervall aktualisiert. Diese Aktualisierungszeit kann entsprechend Ihren Anforderungen an die Bereitstellung von aktualisierten KPIs für das IBM Intelligent Operations Center geändert werden. Weitere Informationen zum Ändern der Eigenschaften in der Tabelle mit Systemeigenschaften erhalten Sie über den Link am Ende des Themas.

Hinweis: Wenn Sie einen KPI im Portlet "Key Performance Indicators (KPIs)" erstellen, werden Aktualisierungen für den KPI nur in Abhängigkeit von der Cacheaktualisierung vorgenommen. Wenn ein KPI in IBM WebSphere Business Monitor definiert wird, kann ein Triggermechanismus definiert werden, um zusätzliche Verarbeitungen als Reaktion auf Änderungen an diesem KPI zu implementieren.

Zugehörige Konzepte:

„Systemweite Konfigurationsdaten angeben” auf Seite 188
In der Tabelle mit den Systemeigenschaften von IBM Intelligent Operations Center sind IBM Intelligent Operations Center-Konfigurationsdaten gespeichert.

Beispiel-KPIs

Im Rahmen des IBM Intelligent Operations Center werden auch Beispiel-KPIs zur Verfügung gestellt. Die Beispiel-KPIs dienen als Anhaltspunkt und sollen Sie bei der Implementierung verschiedener KPI-Typen mit dem IBM WebSphere Business Monitor Development Toolkit unterstützen. Es werden Beispielüberwachungsmodelle aus dem Bereich Wasser, Transport und öffentliche Sicherheit bereitgestellt.

Die KPIs der niedrigsten Ebene werden als Aggregat-KPIs definiert. Aggregat-KPIs werden auf Basis von Werten berechnet, die in eingehenden CAP-Alertnachrichten enthalten sind, sowie auf Basis einer Aggregationsfunktion wie beispielsweise "Durchschnittlich", "Maximal", "Minimal", "Summe", "Häufigkeit" oder "Standardabweichung". Ihre Werte werden als quantifizierbare Messwerte ausgedrückt. KPI-Werte der niedrigeren Ebene werden auf Basis der Ländereinstellung des IBM WebSphere Business Monitor-Servers in das entsprechende Format lokalisiert. Die KPIs der höheren Ebene werden auf Basis der Zuordnungsdefinition bei der Erstellung des Beispiel-KPI den Werten zugeordnet.

Der Wert des Beispiel-KPI einer höheren Ebene ist eine Zahl, die mit einer Farbe und der empfohlenen Reaktionsstufe gleichgesetzt wird. Der Wert "0" ist akzeptabel, der Wert "1" bedeutet "Vorsicht" und beim Wert "2" müssen Maßnahmen ergriffen werden. Der Wert des KPI der niedrigsten Ebene ist eine Dauer, eine Dezimalzahl, ein Prozentsatz oder eine Währung - je nachdem, welchen KPI er darstellt. Beispiel:

- 15% ist der tatsächliche Wert eines KPI, der den Prozentsatz der verspäteten Flüge an einem bestimmten Flughafen über einen gewissen Zeitraum darstellt.
- 5 Minuten, 7 Sekunden ist der tatsächliche Wert eines KPI, der die durchschnittliche Hilfsfrist an einem bestimmten Ort über einen gewissen Zeitraum darstellt.

Die Quellendateien für die Beispielüberwachungsmodelle des IBM Intelligent Operations Center werden in einer Archivdatei zur Verfügung gestellt, die in Rational Application Developer oder WebSphere Integration Developer importiert werden kann, sofern das IBM WebSphere Business Monitor Toolkit installiert ist. Durch die entsprechende Änderung der Archivdatei können KPI-Definitionen geändert, hinzugefügt oder gelöscht werden. Die Definitionen können dann erneut generiert und im IBM Intelligent Operations Center erneut implementiert werden.

Mit dem IBM Intelligent Operations Center werden folgende Beispielmodelle ausgeliefert:

- `icoc_sample_public_safety_monitor_model`
- `icoc_sample_transportation_monitor_model`
- `icoc_sample_water_monitor_model`

Diese Modelle enthalten die folgenden KPI-Beispiele:

- Wasser
  - Hochwasserkontrolle
    - Wasserpegel
      - Durchfluss des Flusses
      - Wasserpegel des Sees
  - Wassermanagement
    - Strategische Planung
      - Wasserverlust
      - Wasserversorgung - Wasserverbrauch

  - Wasserqualität
    - Physikalische Indikatoren
      - Trübung
      - pH
- Verkehr
  - Flughäfen
    - Verspätete Flüge
      - Verspätete Flüge - Flughafen 1
      - Verspätete Flüge - Flughafen 2
  - Straßen und Verkehr
    - Verkehrsereignisse
      - Schwere Unfälle
  - Verkehrswesen
    - Einnahmen
      - Maut für Brücken und Tunnel
      - Parkgebühren
- Öffentliche Sicherheit
  - Feuerwehr
    - Verletzungen bei der Feuerwehr
      - Verletzungen im Dienst - Feuerwache 1
      - Verletzungen im Dienst - Feuerwache 2
  - Polizei
    - Hilfsfrist
      - Hilfsfrist - Bezirk 1
      - Hilfsfrist - Bezirk 2
  - Öffentliche Sicherheit - Planung
    - Öffentliche Sicherheit - Budget
      - Rettungsdienst - Budget
      - Feuerwehr - Budget
      - Polizei - Budget

Zugehörige Konzepte:

„Status" auf Seite 306
Mit dem Portlet "Status" können Sie den Status von KPIs einer einzelnen Einrichtung oder mehrerer Einrichtungen anzeigen.

„Key Performance Indicator - Drilldown" auf Seite 290
Mit dem Portlet "Key Performance Indicator - Drilldown" können Sie weitere Informationen zu einer KPI-Kategorie, den Status der untergeordneten KPIs anzeigen.

„KPIs erstellen und integrieren" auf Seite 116
KPI-Modelle (Key Performance Indicator) können mit einem Entwicklungstoolkit zur Geschäftsüberwachung und einem KPI-Managementportlet erstellt und geändert werden.

„KPIs anpassen" auf Seite 177
Im IBM Intelligent Operations Center können Sie KPI-Modelle (Key Performance Indicator-Modelle) an Ihre Geschäftsprozesse anpassen.

Zugehörige Tasks:

„Monitormodelle implementieren" auf Seite 126
Nach der Definition der KPIs (Key Performance Indicators) und der zugehörigen Monitormodelle müssen die Monitormodelle für den IBM WebSphere Business Monitor implementiert werden, der auf dem Anwendungsserver von IBM Intelligent Operations Center ausgeführt wird.

„Beispielereignisse und KPI-Ereignisse in der Tabelle mit Beispielereignissen anzeigen" auf Seite 115
Das Portlet "Erstellung von Ereignisscripts" veröffentlicht Beispielereignisse aus der Tabelle mit Beispielereignissen in der IBM Intelligent Operations Center-Datenbank. Verwenden Sie die folgende Prozedur, um die Ereignisse in der Tabelle mit Beispielereignissen anzuzeigen.

Tivoli Service Request Manager konfigurieren

In der Benutzerschnittstelle von Tivoli Service Request Manager können Sie Standard Operating Procedures, Workflows und Ressourcen verwalten.

Wenn Sie den Namen von Standard Operating Procedures, Workflows und Ressourcen ein gemeinsames Präfix hinzufügen, ist es einfacher, wenn Sie die Datei in einer Suche filtern. Verwenden Sie beispielsweise für Kundenprojekte das gemeinsame Präfix `CX`.

Sie können angeben, ob die Verbindung zu Tivoli Service Request Manager SSL verwendet, indem Sie die Eigenschaft **`TSRMServerSecurityEnabled`** festlegen. Weitere Informationen zu dieser Eigenschaft und anderen Tivoli Service Request Manager-Eigenschaften erhalten Sie über den Link am Ende des Themas.

Zugehörige Konzepte:

„Ereignisserver" auf Seite 218

„Systemweite Konfigurationsdaten angeben" auf Seite 188
In der Tabelle mit den Systemeigenschaften von IBM Intelligent Operations Center sind IBM Intelligent Operations Center-Konfigurationsdaten gespeichert.

Tivoli Service Request Manager-Benutzerschnittstelle verwenden

Informationen zum Zugriff auf die Tivoli Service Request Manager-Benutzerschnittstelle. Sie können die Verwendung des Tivoli Service Request Manager Start Center vereinfachen und beschleunigen, indem Sie es mit Links zu den häufig verwendeten Funktionen anpassen.

Tivoli Service Request Manager-Anwendungen öffnen

Sie können Tivoli Service Request Manager-Anwendungen in der WebSphere Portal-Verwaltungsschnittstelle entweder über Solution Administration Tools oder über das Portlet "Standard Operating Procedures" öffnen. Sie können eine Ressource in Tivoli Service Request Manager auch über die IBM Intelligent Operations Center-Schnittstelle anzeigen.

Vorbereitende Schritte

Um eine Ressource in Tivoli Service Request Manager über die IBM Intelligent Operations Center-Schnittstelle anzuzeigen, muss die Einzelanmeldung konfiguriert sein.

Vorgehensweise

- Um das Tivoli Service Request Manager Start Center über die WebSphere Portal-Verwaltungsschnittstelle zu öffnen, führen Sie die folgenden Unterschritte aus:
  1. Klicken Sie auf **Intelligent Operations** > **Administration Tools** > **Administration Consoles** (Intelligent Operations > Verwaltungstools > Administrationskonsolen).
  2. Klicken Sie auf **Standard Operating Procedure Administration**.
  3. Melden Sie sich als Administrator beim Tivoli Service Request Manager Start Center an.
- Um Tivoli Service Request Manager-Anwendungen zu öffnen, die in Bezug zu Standard Operating Procedures stehen, verwenden Sie das Portlet "Standard Operating Procedures":
  1. Um das Portlet "Standard Operating Procedures" zu öffnen, klicken Sie in der Verwaltungsschnittstelle von WebSphere Portal auf **Intelligent Operations** > **Customization Tools** > **Standard Operating Procedures** (Intelligent Operations > Anpassungstools > Standard Operating Procedures).
  2. Wählen Sie eine der folgenden Optionen aus:
     - Um die Anwendung "Standard Operating Procedure" zu öffnen, klicken Sie auf **Standard Operating Procedures**.
     - Um die Anwendung "Auswahlmatrix für Standard Operating Procedures" zu öffnen, klicken Sie auf **Auswahlmatrix für Standard Operating Procedures**.
     - Um die Anwendung "Workflow-Designer" zu öffnen, klicken Sie auf **Workflow-Designer**.
- Um eine Ressource in der Tivoli Service Request Manager-Benutzerschnittstelle über die IBM Intelligent Operations Center-Schnittstelle anzuzeigen, führen Sie die folgenden Schritte aus:
  1. Klicken Sie im Portlet "Details" auf der Registerkarte **Ereignisse und Vorfälle** mit der rechten Maustaste auf eine Zeile in der Ereignisliste.
  2. Soll eine Liste der Ressourcen im näheren Umfeld des Ereignisses angezeigt werden, klicken Sie auf **Ressourcen in der Nähe anzeigen** und wählen Sie den Radius des gewünschten Bereichs aus. Auf der Registerkarte **Ressourcen** wird eine Liste mit Ressourcen angezeigt.
  3. Klicken Sie auf der Registerkarte **Ressourcen** mit der rechten Maustaste auf eine Zeile in der Ressourcenliste und anschließend auf **Eigenschaften**. Die Ressource wird in Tivoli Service Request Manager auf der Registerkarte **Ressourcen** angezeigt.

  Anmerkung: Um sich von Tivoli Service Request Manager vollständig abzumelden, müssen Sie das Web-Browser-Fenster mit der Tivoli Service Request Manager-Benutzerschnittstelle schließen.

Zugehörige Tasks:

„Single Sign-on für Services zur Zusammenarbeit konfigurieren” auf Seite 57
Importieren Sie das WebSphere Portal SSO LTPA-Token in den Ereignisserver, um es Benutzern zu ermöglichen, auf die Services zur Zusammenarbeit zuzugreifen, ohne dass sie ihre Identifikationsdaten erneut eingeben müssen.

Bevorzugte Anwendungen im Tivoli Service Request Manager Start Center einrichten

Aktualisieren Sie Ihre bevorzugten Anwendungen im Tivoli Service Request Manager Start Center, damit Sie einfacher darauf zugreifen können.

Informationen zu diesem Vorgang

Jedem Tivoli Service Request Manager-Benutzer steht sein eigenes Tivoli Service Request Manager Start Center mit einer angepassten Liste unter "Bevorzugte Anwendungen" zur Verfügung.

Vorgehensweise

1. Um das Tivoli Service Request Manager Start Center oben in der Tivoli Service Request Manager-Benutzerschnittstelle anzuzeigen, klicken Sie auf **Startcenter**.
2. Klicken Sie im Tivoli Service Request Manager Start Center auf das Symbol **Portlet bearbeiten** neben "Bevorzugte Anwendungen".
3. Klicken Sie im Fenster **Favorite Applications Setup** (Bevorzugte Anwendungen einrichten) auf **Anwendungen auswählen**.
4. Wählen Sie im Fenster **Anwendungen auswählen** die Anwendungen aus, die unter "Bevorzugte Anwendungen" angezeigt werden sollen . In der folgenden Liste werden die Anwendungen angezeigt, die für IBM Intelligent Operations Center-Benutzer hilfreich sind:

   CRONTASK
   Konfiguration der Crontask

   DOMAINADM
   Domänen

   PERSON
   Personen

   PERSONGR
   Personengruppen

   PLUSIMTRIX
   Auswahlmatrix für Standard Operating Procedures

   PLUSIRES
   Ressourcen

   PLUSIWO
   SOP-Aktivitäten

   USER Benutzer

   WFDESIGN
   Workflow-Designer
5. Führen Sie die folgenden Schritte aus, um die Position zu definieren, an der Anwendungen unter "Bevorzugte Anwendungen" aufgelistet sind:
   a. Wählen Sie im Fenster **Favorite Applications Setup** (Bevorzugte Anwendungen einrichten) eine Anwendung aus.
   b. Geben Sie im Feld **Reihenfolge** eine Nummer ein.
6. Klicken Sie zum Speichern der Aktualisierungen auf **Fertig**.

Neue Benutzer in Tivoli Service Request Manager konfigurieren

Wenn Sie einen Benutzer in IBM Intelligent Operations Center hinzufügen, ordnen Sie Berechtigungen und Personengruppen für den Benutzer in Tivoli Service Request Manager zu.

Die Standardeinfügesite festlegen

Damit ein neuer Benutzer neue Ressourcen hinzufügen und Standard Operating Procedures anwenden kann, müssen Sie die Standardeinfügesite für den Benutzer festlegen.

Vorgehensweise

1. Melden Sie sich als Administrator beim Tivoli Service Request Manager Start Center an.
2. Klicken Sie auf **Go to** > **Security** > **Users** (Weiter mit > Sicherheit > Benutzer).
3. Um den Benutzer zu suchen, geben Sie in der Registerkarte **List** im Feld **User** einige oder alle Buchstaben im Namen des Benutzers ein.

4. Klicken Sie in der Liste auf den Namen des Benutzers und klicken Sie anschließend auf die Registerkarte **User**.
5. Klicken Sie unter Benutzereinstellungen neben dem Feld **Default Insert Site** (Standardeinfügesite) auf das Symbol **Wert auswählen**.
6. Suchen Sie im Fenster **Wert auswählen** den Namen der Standardeinfügesite und klicken Sie darauf; z. B. **PMSCRTP**. PMSCRTP ist eine Beispielsite, die mit dem IBM Intelligent Operations Center installiert wird.
7. Klicken Sie auf das Symbol **Save User** (Benutzer speichern).

Einen Benutzer einer Sicherheitsgruppe zuordnen

Fügen Sie Benutzer den entsprechenden Sicherheitsgruppen hinzu, damit sie auf die entsprechenden Anwendungen in Tivoli Service Request Manager Zugriff haben.

Informationen zu diesem Vorgang

Verwenden Sie die folgende Prozedur, um einen Benutzer einer Gruppe zuzuordnen.

Vorgehensweise

1. Melden Sie sich als Administrator beim Tivoli Service Request Manager Start Center an.
2. Klicken Sie auf **Go To** > **Security** > **Users** (Weiter mit > Sicherheit > Benutzer).
3. Um den Benutzer zu suchen, geben Sie in der Registerkarte **List** im Feld **User** einige oder alle Buchstaben im Namen des Benutzers ein.
4. Klicken Sie in der Liste auf den Namen des Benutzers und klicken Sie anschließend auf die Registerkarte **Groups**.
5. Um die Gruppe zu suchen, der Sie den Benutzer hinzufügen möchten, geben Sie im Feld **Group** einige oder alle Buchstaben im Namen der Gruppe ein.
6. Wenn der Name der erforderlichen Gruppe nicht in der Liste enthalten ist, klicken Sie auf **New Row** (Neue Zeile).
7. Klicken Sie unter "Details" neben dem Feld **Group** auf das Symbol **Detail Menu** (Detailmenü) und anschließend auf **Select Value** (Wert auswählen).
8. Suchen Sie im Fenster **Select Value** (Wert auswählen) den Namen der erforderlichen Gruppe und klicken Sie darauf.
9. Klicken Sie auf das Symbol **Save User** (Benutzer speichern).

Einen Benutzer einer Personengruppe zuordnen

In einer Standard Operating Procedure können die Tasks vordefinierten Personengruppen zugeordnet werden. Ein Benutzer muss Mitglied einer bestimmten Personengruppe sein, damit er die Tasks anzeigen kann, die dieser Personengruppe zugeordnet sind.

Vorbereitende Schritte

Sie können entweder die Personengruppen verwenden, die bei der Installation von IBM Intelligent Operations Center als Beispiele bereitgestellt werden, oder Sie können Ihre eigenen Personengruppen erstellen. Informationen zum Erstellen einer Personengruppe in Tivoli Service Request Manager finden Sie im Information Center für Maximo Asset Management.

Anmerkung: Stellen Sie sicher, dass die Namen aller Personengruppen dieselbe Länge aufweisen. Damit stellen Sie sicher, dass Benutzern nur Tasks zugeordnet werden, die den Personengruppen zugeordnet sind, bei denen sie Mitglieder sind.

Informationen zu diesem Vorgang

Verwenden Sie die folgende Prozedur, um einen Benutzer einer Personengruppe zuzuordnen.

Vorgehensweise

1. Melden Sie sich als Administrator beim Tivoli Service Request Manager Start Center an.
2. Klicken Sie auf **Go To** > **Administration** > **Resources** > **Person Groups** (Weiter mit > Administration > Ressourcen > Personengruppen).
3. Um die erforderliche Personengruppe zu suchen, geben Sie auf der Registerkarte **List** im Feld **Person Groups** einige oder alle Buchstaben im Namen der Personengruppe ein.
4. Klicken Sie in der Liste auf den Namen der Personengruppe.
5. Klicken Sie auf der Registerkarte **Person Group** (Personengruppe) unter "People" (Personen) auf **New Row** (Neue Zeile).
6. Klicken Sie unter "Details" neben dem Feld **Person** auf das Symbol **Detail Menu** (Detailmenü) und anschließend auf **Select Value** (Wert auswählen).
7. Suchen Sie im Fenster **Select Value** (Wert auswählen) den Namen des Benutzers, den Sie zur Personengruppe hinzufügen möchten, und klicken Sie darauf.
8. Geben Sie im Feld **Sequence** (Folge) die nächste verfügbare inkrementelle Zahl ein.
9. Klicken Sie auf das Symbol **Save Person Group** (Personengruppe speichern).

Zugehörige Informationen:

Information Center für Maximo Asset Management

Standard Operating Procedures

Für die Verwaltung von Ereignissen, die im IBM Intelligent Operations Center auftreten, können Sie Standard Operating Procedures und Aktivitäten definieren. Verwenden Sie das Portlet "Standard Operating Procedures", um auf Standard Operating Procedure, Auswahlmatrix für Standard Operating Procedure und Workflow-Designer-Anwendungen in Tivoli Service Request Manager zuzugreifen.

Starten Sie das Portlet "Standard Operating Procedures", indem Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Customization Tools** > **Standard Operating Procedures** (Intelligent Operations > Anpassungstools > Standard Operating Procedures) klicken.

Über eine Standard Operating Procedure werden eine Reihe von Aktivitäten definiert, deren Ausführung durch ein Ereignis ausgelöst wird, dessen Parameter vordefinierte Bedingungen erfüllen; dabei entspricht jede Aktivität einer manuellen oder einer automatischen Task. Einer automatischen Task kann ein Workflow zugeordnet werden. Jede Aktivität ist einer Eignergruppe zugeordnet; Benutzer werden Eignergruppen über ihre Zugehörigkeit zu einer Personengruppe zugeordnet. Alle Benutzer, die zu der Eignergruppe gehören, können die Aktivitäten über das Portlet "Meine Aktivitäten" verwalten.

Sie können die Reihenfolge vorgeben, in der ein Teil oder alle der Aktivitäten in einer Standard Operating Procedure ausgeführt werden sollen. So können Sie beispielsweise vorgeben, dass eine bestimmte Aktivität erst ausgeführt wird, wenn die vorangehende Aktivität abgeschlossen oder aber übersprungen wurde.

Um die Standard Operating Procedure-Anwendung zu öffnen, klicken Sie im Portlet "Standard Operating Procedures" auf **Standing Operating Procedures**.

Auswahlmatrix für Standard Operating Procedure

In der Auswahlmatrix für Standard Operating Procedure werden die Ereignisparameter definiert, die vorgeben, ob eine Standard Operating Procedure für ein bestimmtes Ereignis eingeleitet wird. Jede Standard Operating Procedure kann über eine oder mehrere Gruppen mit Auswahlkriterien verfügen. Jede Gruppe mit Auswahlkriterien muss jedoch eindeutig sein.

Um die Auswahlmatrix für Standard Operating Procedure zu öffnen, klicken Sie im Portlet "Standard Operating Procedures" auf **Auswahlmatrix der Standard Operating Procedures**.

Workflow-Designer

Mit dem Workflow-Designer können Sie Workflows gestalten, die den Standard Operating Procedure-Aktivitäten als automatische Tasks hinzugefügt werden können.

Um die Workflow-Designer-Anwendung zu öffnen, klicken Sie im Portlet "Standard Operating Procedures" auf **Workflow-Designer**.

Portlet "Standard Operating Procedures" anpassen

Sie haben die Möglichkeit, dieses Portlet anzupassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Zugehörige Konzepte:

„Meine Aktivitäten” auf Seite 300
Im Portlet "Meine Aktivitäten" wird eine dynamische Liste mit Aktivitäten angezeigt, deren Eigner die Gruppe ist, zu der der an der Schnittstelle angemeldete Benutzer gehört.

Zugehörige Verweise:

„Einstellungen des Standard Operating Procedures-Portlets” auf Seite 174
Anpassen des Standard Operating Procedures-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Workflows erstellen

In Tivoli Service Request Manager können Sie Workflows erstellen, die Sie als automatische Tasks in Ihre Standard Operating Procedure-Aktivitäten einschließen können.

Informationen zu diesem Vorgang

Detaillierte Informationen zum Erstellen von Workflows erhalten Sie über den Link zum Information Center für Maximo Asset Management am Ende des Themas.

Vorgehensweise

1. Um das Portlet "Standard Operating Procedures" zu öffnen, klicken Sie in der Verwaltungsschnittstelle von WebSphere Portal auf **Intelligent Operations** > **Customization Tools** > **Standard Operating Procedures** (Intelligent Operations > Anpassungstools > Standard Operating Procedures).
2. Um die Anwendung "Workflow-Designer" zu öffnen, klicken Sie auf **Workflow-Designer**.
3. Klicken Sie im Fenster **Workflow-Designer** auf die Registerkarte **Canvas** (Bereich).
4. Klicken Sie auf der Registerkarte **Canvas** (Bereich) auf die entsprechenden Symbole zum Einfügen der erforderlichen Knoten und Pfeile für den Workflow.

Zugehörige Informationen:


Information Center für Maximo Asset Management

Standard Operating Procedures erstellen

Erstellen Sie eine Standard Operating Procedure und ordnen Sie sie einer Eignergruppe zu. Benutzer werden Eignergruppen über ihre Zugehörigkeit zu einer Personengruppe zugeordnet.

Vorgehensweise

1. Um das Portlet "Standard Operating Procedures" zu öffnen, klicken Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Customization Tools** > **Standard Operating Procedures** (Intelligent Operations > Anpassungstools > Standard Operating Procedures).
2. Klicken Sie zum Öffnen der Anwendung Standard Operating Procedure auf **Standard Operating Procedures**.

3. Klicken Sie im Fenster **Standard Operating Procedure** auf der Registerkarte **List** (Liste) auf das Symbol **New SOP** (Neue SOP). Auf der Registerkarte **Standard Operating Procedure** wird eine leere Standard Operating Procedure angezeigt.
4. Geben Sie für **SOP Name** einen Namen ein und geben Sie im Feld neben **SOP Name** eine Beschreibung ein. Verwenden Sie für die Namen von Standard Operating Procedures ein einheitliches Format ähnlich den Namen des Beispiels für Standard Operating Procedures; z. B. `Vorbereitung für Evakuierung aufgrund von Unwetter (Vorbereitung)`. Ebenso gilt: Fügen Sie das LRM-Zeichen ein, wenn das letzte Zeichen des Namens eine rechte runde Klammer ist, um potenzielle Probleme bei der Darstellung von bidirektionalem Text zu vermeiden. Geben Sie z. B. den im vorherigen Beispiel als `Vorbereitung für Evakuierung aufgrund von Unwetter (Vorbereitung)&#x200E;` verwendeten Namen ein. Das LRM-Zeichen wird nach dem Speichern von Standard Operating Procedure in der Benutzerschnittstelle nicht angezeigt.Wenn Sie zu allen Namen Ihrer Standard Operating Procedures ein gemeinsames Präfix hinzufügen, lassen sich Ihre Standard Operating Procedures bei Suchvorgängen auch leichter filtern. Verwenden Sie beispielsweise für Kundenprojekte das gemeinsame Präfix `CX`.
5. Um eine Langbeschreibung einzugeben, klicken Sie auf das Symbol neben dem Beschreibungsfeld, und geben Sie im angezeigten Fenster eine Beschreibung ein.
6. Wählen Sie unter "Details" in der Liste **Template Type** (Vorlagentyp) die Option **Activity** (Aktivität) aus.
7. Ordnen Sie unter "Details" der Standard Operating Procedure eine Eignergruppe zu:
   a. Klicken Sie auf das Symbol neben dem Feld **Owner Group** (Eignergruppe).
   b. Klicken Sie im Fenster **Select Value** (Wert auswählen) auf einen Wert in der Liste, um ihn auszuwählen.
8. Optional: Geben Sie für **Duration** (Dauer) einen Zeitraum ein, in dem die Standard Operating Procedure abgeschlossen werden muss. Das Format für die Eingabe des Zeitraums lautet *hh*:*mm*, wobei *hh* die Anzahl der Stunden und *mm* die Anzahl der Minuten angibt. Das Fälligkeitsdatum wird auf Grundlage der Ausführungsdauer berechnet.
9. Fügen Sie der Standard Operating Procedure nach Bedarf Tasks hinzu:
   a. Klicken Sie in der rechten unteren Ecke der Tivoli Service Request Manager-Benutzerschnittstelle auf **New Row** (Neue Zeile). Unter "SOP Steps" wird der Liste der Tasks eine neue Taskzeile hinzugefügt.
   b. Geben Sie für **Sequence** (Folge) und für **Task** dieselbe Nummer ein. Nummerieren Sie Tasks nach dem folgenden Muster: `10`, `20`, `30` usw. Durch dieses Muster haben Sie später mehr Flexibilität, um Tasks hinzuzufügen oder zu entfernen.
   c. Geben Sie für **Instruction** (Anweisung) eine Taskbeschreibung an. Um eine der zuvor eingegebenen Beschreibungen auszuwählen, klicken Sie auf das Symbol neben dem Beschreibungsfeld.
   d. Optional: Workflow zuordnen:
      1) Klicken Sie bei **Workflow Name** auf das Symbol **Select Value** (Wert auswählen).
      2) Klicken Sie im Fenster **Select Value** (Wert auswählen) auf einen Wert in der Liste, um ihn auszuwählen. Geben Sie im Filterfeld, das oberhalb der Liste angezeigt wird, die ersten Buchstaben des Workflows ein, den Sie verwenden möchten, um die Liste einzugrenzen.
      3) Erweitern Sie die Taskzeile und geben Sie unter "Details" weitere erforderliche Einzelheiten ein. Bei Bedarf können Sie eine Eignergruppe und Ablaufsteuerungseinstellungen angeben. Wenn Sie keine Eignergruppe und Ablaufsteuerungseinstellungen für die Task angeben, erbt die Task die Einstellungen von der übergeordneten Standard Operating Procedure.
10. Um die Standard Operating Procedure zu speichern, klicken Sie im oberen Bereich der Tivoli Service Request Manager-Benutzerschnittstelle auf das Symbol **Save SOP** (SOP speichern).
11. Um die Standard Operating Procedure auf die in der Auswahlmatrix für Standard Operating Procedure angegebenen Ereignisse anwenden zu können, stellen Sie sicher, dass der Status von `DRAFT` in `ACTIVE` geändert wurde:
    a. Klicken Sie auf das Symbol **Change Status** (Status ändern).

b. Wählen Sie im Fenster **Change Status** aus der Liste unter **New Status** den Status **Active** aus.
c. Optional: Geben Sie für **As Of Date** und **Memo** Werte ein.
d. Klicken Sie auf **OK**.

12. Führen Sie die folgenden Schritte aus, um die verfügbaren Standard Operating Procedures zu überprüfen:
    a. Klicken Sie auf die Registerkarte **List** (Liste).
    b. Wählen Sie unter "SOP Job Plans" eine der folgenden Optionen aus:
        - Drücken Sie im Filterfeld die Eingabetaste, um alle verfügbaren Standard Operating Procedures anzuzeigen.
        - Geben Sie im Filterfeld die ersten Buchstaben des Namens einer Standard Operating Procedure ein.
    c. Um die Details zu einer Standard Operating Procedure anzuzeigen, klicken Sie in der Liste auf den Namen der Standard Operating Procedure. Die Details werden auf der Registerkarte **Standard Operating Procedure** angezeigt.

Nächste Schritte

Wenn Sie die Reihenfolge festlegen möchten, in der einige oder alle Aktivitäten in einer Standard Operating Procedure ausgeführt werden sollen, wählen Sie unter "Details" das Kontrollkästchen **Flow Controlled?** aus. Weitere Informationen zum Festlegen der Reihenfolge der Aktivitäten, die Benutzern oder Gruppen auf der Grundlage von Standard Operating Procedures zugeordnet werden, finden Sie im Information Center zu Maximo Asset Management. Suchen Sie dort nach *flow control*.

Definieren Sie in der Auswahlmatrix für Standard Operating Procedure die Ereignisparameter, die bestimmen, für welche Ereignisse die Standard Operating Procedure ausgewählt wird.

Zugehörige Tasks:

„Einen Benutzer einer Personengruppe zuordnen" auf Seite 134
In einer Standard Operating Procedure können die Tasks vordefinierten Personengruppen zugeordnet werden. Ein Benutzer muss Mitglied einer bestimmten Personengruppe sein, damit er die Tasks anzeigen kann, die dieser Personengruppe zugeordnet sind.

Zugehörige Informationen:

Information Center für Maximo Asset Management

Einträge in der Auswahlmatrix für Standard Operating Procedure überprüfen

Überprüfen Sie in der Auswahlmatrix für Standard Operating Procedure die Auswahlkriterien für jede Standard Operating Procedure. Die Auswahlkriterien basieren auf Ereignisparametern.

Vorgehensweise

1. Um das Portlet "Standard Operating Procedures" zu öffnen, klicken Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Customization Tools** > **Standard Operating Procedures** (Intelligent Operations > Anpassungstools > Standard Operating Procedures).
2. Um die Anwendung "Auswahlmatrix für Standard Operating Procedures" zu öffnen, klicken Sie auf **Auswahlmatrix für Standard Operating Procedures**.
3. Klicken Sie im Fenster **Auswahlmatrix für Standard Operating Procedures** auf das Symbol **Filter**, um die Filterzeile anzuzeigen.
4. Legen Sie fest, welches Filterfeld verwendet werden soll:
    - Kategorie
    - Schweregrad
    - Dringlichkeit
    - Gewissheit

- Name der SOP

5. Wählen Sie eine der folgenden Optionen aus:
   - Drücken Sie im Filterfeld die Eingabetaste, um alle vorhandenen Einträge anzuzeigen, die zum ausgewählten Parameter oder zum Namen der Standard Operating Procedure in Beziehung stehen.
   - Geben Sie im Filterfeld die ersten Buchstaben eines Wertes an, mit dem gefiltert werden soll.
   - Wenn Sie mit einem Parameterwert filtern, geben Sie den Wert über das Fenster **Select Value** (Wert auswählen) ein:
     a. Klicken Sie neben dem Filterfeld auf das Symbol **Select Value**.
     b. Klicken Sie im Fenster **Select Value** (Wert auswählen) auf einen Wert in der Liste, um ihn auszuwählen.
   - Gehen Sie wie folgt vor, um über das Fenster **Standard Operating Procedure** den Namen einer Standard Operating Procedure auszuwählen, mit dem gefiltert werden soll:
     a. Klicken Sie neben dem Filterfeld **SOP NAME** auf das Symbol **Detail Menu** und klicken Sie anschließend auf **Go To Standard Operating Procedure**.
     b. Klicken Sie im Fenster **Standard Operating Procedure** auf die Registerkarte **List** (Liste).
     c. Geben Sie im Filterfeld unter "SOP Job Plans" die ersten Buchstaben des Namens einer Standard Operating Procedure ein.
     d. Um die Details zu einer Standard Operating Procedure anzuzeigen, klicken Sie in der Liste auf den Namen der Standard Operating Procedure. Die Details werden auf der Registerkarte **Standard Operating Procedure** angezeigt.
     e. Um den Namen der Standard Operating Procedure, der auf der Registerkarte **Standard Operating Procedure** angezeigt wird, zurückzugeben, klicken Sie in der rechten oberen Ecke auf **Return With Value**. Der Name wird im Filterfeld **SOP Name** in der Auswahlmatrix angezeigt.
6. Um die Liste der angezeigten Einträge zu Auswahlkriterien weiter einzugrenzen, wiederholen Sie Schritt 5 mit einem der in Schritt 4 aufgeführten Filterfelder.

Parameter in der Auswahlmatrix für Standard Operating Procedure definieren

Definieren Sie in der Auswahlmatrix für Standard Operating Procedure die Ereignisparameter, die bestimmen, ob eine Standard Operating Procedure für ein bestimmtes Ereignis ausgewählt wird.

Informationen zu diesem Vorgang

Sie können keine Auswahlmatrix für Standard Operating Procedure speichern, die zwei Zeilen mit identischen Auswahlkriterien enthält. Es wird ggf. eine Auswertungsnachricht angezeigt, um Sie darüber zu informieren, dass Sie für eine Standard Operating Procedure eindeutige Auswahlkriterien festlegen müssen.

Vorgehensweise

1. Um das Portlet "Standard Operating Procedures" zu öffnen, klicken Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Customization Tools** > **Standard Operating Procedures** (Intelligent Operations > Anpassungstools > Standard Operating Procedures).
2. Um die Anwendung "Auswahlmatrix für Standard Operating Procedures" zu öffnen, klicken Sie auf **Auswahlmatrix für Standard Operating Procedures**.
3. Klicken Sie im Fenster **Auswahlmatrix für Standard Operating Procedures** auf das Symbol **Filter**, um die Filterzeile anzuzeigen.
4. Klicken Sie im Fenster **Auswahlmatrix für Standard Operating Procedures** in der rechten unteren Ecke auf **New Row**. Es wird eine neue Zeile zu der Auswahlmatrix hinzugefügt.
5. Geben Sie für jeden der folgenden Parameter einen Wert ein:
   - Kategorie
   - Schweregrad
   - Dringlichkeit
   - Gewissheit

Verwenden Sie eine der folgenden Optionen, um für jeden der Parameter einen Wert einzugeben:

- Gehen Sie wie folgt vor, um Werte über das Fenster **Select Value** (Wert auswählen) einzugeben:
  a. Klicken Sie neben dem Parameterfeld auf das Symbol **Select Value**.
  b. Klicken Sie im Fenster **Select Value** (Wert auswählen) auf einen Wert in der Liste, um ihn auszuwählen.
- Gehen Sie wie folgt vor, um den Namen des Parameters manuell einzugeben:
  a. Geben Sie im Feld die ersten Buchstaben des Parameterwertes ein.
  b. Drücken Sie die Tabulatortaste, um den Cursor in das nächste Feld zu verschieben; der Parameterwert wird automatisch vervollständigt.

6. Wählen Sie eine der folgenden Optionen aus, um den Namen der Standard Operating Procedure im Feld **SOP Name** einzugeben:
   - Gehen Sie wie folgt vor, um den Namen der Standard Operating Procedure über das Fenster **Standard Operating Procedure** einzugeben:
     a. Klicken Sie neben dem Feld **SOP NAME** auf das Symbol **Detail Menu** und klicken Sie anschließend auf **Go To Standard Operating Procedure**.
     b. Klicken Sie im Fenster **Standard Operating Procedure** auf die Registerkarte **List** (Liste).
     c. Geben Sie im Filterfeld unter "SOP Job Plans" die ersten Buchstaben des Namens einer Standard Operating Procedure ein.
     d. Um die Details zu einer Standard Operating Procedure anzuzeigen, klicken Sie in der Liste auf den Namen der Standard Operating Procedure. Die Details werden auf der Registerkarte **Standard Operating Procedure** angezeigt.
     e. Um den Namen der Standard Operating Procedure, der auf der Registerkarte **Standard Operating Procedure** angezeigt wird, zurückzugeben, klicken Sie in der rechten oberen Ecke auf **Return With Value**. Der Name wird im Feld **SOP Name** in der neuen Zeile der Auswahlmatrix angezeigt.
   - Geben Sie den Namen der Standard Operating Procedure manuell ein.
7. Klicken Sie auf das Symbol **Save matrix** (Matrix speichern).

Ressourcen verwalten

Verwalten Sie Ihre Ressourcen in Tivoli Service Request Manager.

Beispielressourcen mit der IBM Intelligent Operations Center-Datenbank synchronisieren

Wenn Sie die Beispielressourcen verwenden möchten, die mit IBM Intelligent Operations Center installiert sind, müssen Sie sie mit der IBM Intelligent Operations Center-Datenbank manuell synchronisieren.

Vorgehensweise

1. Melden Sie sich als Administrator beim Tivoli Service Request Manager Start Center an.
2. Klicken Sie auf **Go to** > **Assets** > **IOC Resources (IntOpCtr)** (Weiter mit > Assets > IOC-Ressourcen (IntOpCtr)).
3. Um alle IBM Intelligent Operations Center-Beispielressourcen anzuzeigen, klicken Sie im Fenster **Resources (IntOpCtr)** auf der Registerkarte **List** auf das Feld **Resource** und drücken Sie anschließend die Eingabetaste.
4. Aktualisieren Sie die Ressource für jede Ressource, die Sie mit der IBM Intelligent Operations Center-Datenbank synchronisieren möchten. Beispiel: Ändern Sie die **Beschreibung** und speichern Sie die Änderung.
5. Prüfen Sie, ob die synchronisierten Ressourcen in den folgenden IBM Intelligent Operations Center-Datenbanktabellen aufgelistet ist:
   - `IOC.RESOURCE`
   - `IOC.RESOURCE_X_CAPABILITY`

Nächste Schritte

Wenn die Beispielressourcen nicht korrekt mit der IBM Intelligent Operations Center-Datenbank synchronisiert sind, prüfen Sie die Tivoli Netcool/Impact-Prüfprotokolldatei. Geben Sie den folgenden Befehl ein:

```
tail –f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

Prüfen Sie auch die Tivoli Netcool/Impact-Richtlinienprotokolldatei unter `/opt/IBM/netcool/impact/log/NCI_policylogger.log`. Führen Sie die folgenden Schritte aus, um die Tivoli Netcool/Impact-Richtlinienprotokolldatei zu aktivieren:

1. Melden Sie sich bei der Tivoli Netcool/Impact-Administrationskonsole unter `http://event_server:9080/nci` an. Melden Sie sich als Benutzer `admin` mit dem Kennwort `netcool` an.
2. Klicken Sie auf **IOC Project** (IOC-Projekt).
3. Klicken Sie auf der Registerkarte **Services** auf **Policy Logger** (Richtlinienprotokollfunktion).
4. Ändern Sie für **Highest Level Log** (Protokoll der höchsten Ebene) den Wert von `0` in `3`.
5. Speichern Sie die Änderungen.
6. Führen Sie den Test aus.

Weitere Informationen zur Fehlersuche in Protokolldateien erhalten Sie über den Link am Ende des Themas.

Zugehörige Konzepte:

„Protokolldateien des Ereignisservers” auf Seite 312
Mit den folgenden Prozeduren können Sie für einige der Systeme auf dem Ereignisserver das Tracing aktivieren und Protokolle anzeigen.

Ereigniskategorie/Funktion-Zuordnung erstellen oder ändern

Ressourcen werden im Portlet "Karte" in Abhängigkeit von der Kategorie des ausgewählten Ereignisses und von den zugeordneten Ressourcenfunktionen angezeigt. Bevor Sie eine Ressource erstellen, ordnen Sie die Funktion der Ressource der entsprechenden Ereigniskategorie zu.

Vorbereitende Schritte

Um sicherzustellen, dass die Ressourcenfunktionen aktualisiert werden, müssen Sie den Wert des Kennworts für den Tivoli Service Request Manager-Benutzer mit Verwaltungsaufgaben, z. B. **`maxadmin`**, auf `maxadmin` setzen.

Informationen zu diesem Vorgang

Mit der Zuordnung einer Ressourcenfunktion zu einer Ereigniskategorie wird sichergestellt, dass beim Anzeigen von Ressourcen in der Nähe im Portlet "Details" von IBM Intelligent Operations Center die entsprechenden Ressourcen im Portlet "Karte" angezeigt werden. Beispiel: Wenn Sie Ressourcen in der Nähe für eine meteorologische Ereigniskategorie anzeigen, wird ein Lager mit Sandsäcken angezeigt, wobei das Lager der Ressourcentyp ist und die Sandsäcke eine zugeordnete Funktion des Lagers sind.

Vorgehensweise

1. Melden Sie sich als Administrator beim Tivoli Service Request Manager Start Center an.
2. Klicken Sie auf **Go to** > **System Configuration** > **Platform Configuration** > **Domains** (Weiter mit > Systemkonfiguration > Plattformkonfiguration > Domänen).
3. Wählen Sie die entsprechende Option aus:
   - Um eine neue Ereigniskategorie/Funktion-Zuordnung zu erstellen, klicken Sie auf **New Row** (Neue Zeile) und geben Sie die entsprechenden Details in die Felder ein.
   - Um eine bestehende Ereigniskategorie/Funktion-Zuordnung zu ändern, verwenden Sie das Filterfeld, um die entsprechenden Ereigniskategoriezuordnungen anzuzeigen, klicken Sie anschließend auf die zu bearbeitende Zeile und ändern Sie die Details.

- Um eine bestehende Ereigniskategorie/Funktion-Zuordnung zu löschen, verwenden Sie das Filterfeld, um die entsprechenden Ereigniskategoriezuordnungen anzuzeigen, klicken Sie anschließend auf das Symbol **Mark Row for Delete** (Zeile zum Löschen markieren) am Ende der zu löschenden Zeile.

4. Klicken Sie auf das Symbol **Save Domain** (Domäne speichern).
5. Prüfen Sie, ob die zugeordneten Ressourcen in den folgenden IBM Intelligent Operations Center-Datenbanktabellen aufgelistet ist:
   - `IOC.RESOURCE`
   - `IOC.RESOURCE_X_CAPABILITY`

Ergebnisse

Neue Ressourcen, deren Funktion der Ereigniskategorie des aktuell ausgewählten Ereignisses zugeordnet ist, werden sofort im Portlet "Karte" von IBM Intelligent Operations Center angezeigt. Aktualisierte Ressourcen, deren Funktion der Ereigniskategorie des aktuell ausgewählten Ereignisses zugeordnet ist, werden nur angezeigt, nachdem die Seite mit dem Portlet "Karte" von IBM Intelligent Operations Center neu geladen wurde.

Nächste Schritte

- Wenn die zugeordneten Ressourcen nicht korrekt in der IBM Intelligent Operations Center-Datenbank aufgelistet sind, prüfen Sie die Tivoli Netcool/Impact-Protokolldatei. Geben Sie den folgenden Befehl ein:

  ```
  tail –f /opt/IBM/netcool/omnibus/log/ioc_xml.log
  ```

  Weitere Informationen zur Fehlersuche in Protokolldateien erhalten Sie über den Link am Ende des Themas.
- Wenn Sie einer Funktion mehr als zwei Ereigniskategorien zuordnen möchten, verwenden Sie einen DB2-Befehl, um die Zuordnung auszuführen. Verwenden Sie die folgenden Schritte:
  1. Geben Sie den folgenden Befehl ein, um sich beim Datenserver als Tivoli Service Request Manager-Datenbankbenutzer anzumelden: `su - db2inst6`
  2. Geben Sie folgenden Befehl ein, um eine Verbindung zur IBM Intelligent Operations Center-Datenbank herzustellen: `db2 connect to maximo`
  3. Geben Sie folgenden Befehl ein, um einer Funktion eine Ereigniskategorie zuzuordnen:

     ```
     insert into synonymdomain
     (domainid, maxvalue, value, description, defaults, synonymdomainid, valueid) values
     ('PLUSICATCPLMAP', 'Kategoriename', 'Funktionsname',
     'Zuordnungsbeschreibung', 0,   NEXTVAL FOR synonymdomainseq,
     'PLUSICATCPLMAP|Zuordnungsschlüssel');
     ```

     Ersetzen Sie im vorherigen Befehl die Variablen *Kategoriename*, *Funktionsname*, *Zuordnungsbeschreibung* und *Zuordnungsschlüssel* durch die entsprechenden Werte. Erstellen Sie einen geeigneten Wert für *Zuordnungsschlüssel*. Beispiel: Mit dem folgenden Befehl wird der Funktion `COT` die Ereigniskategorie `Met` zugeordnet und dem *Zuordnungsschlüssel* wird der Wert `METCOT` zugeordnet.

     ```
     insert into synonymdomain
     (domainid, maxvalue, value, description, defaults, synonymdomainid, valueid) values
     ('PLUSICATCPLMAP', 'Met', 'COT', 'Has cots', 0,   NEXTVAL FOR synonymdomainseq,
     'PLUSICATCPLMAP|METCOT');
     ```
  4. Geben Sie folgenden Befehl ein, um den Schreibvorgang in die Datenbank abzuschließen: `db2 commit;`

Ressource erstellen

Erstellen Sie eine Ressource in der Tivoli Service Request Manager-Benutzerschnittstelle.

Vorbereitende Schritte

Stellen Sie sicher, dass die Funktionalität der neuen Ressource einer Kategorie zugeordnet ist, sodass die Ressource im Portlet "Karte" in der IBM Intelligent Operations Center-Benutzerschnittstelle angezeigt wird.

Vorgehensweise

1. Melden Sie sich als Administrator beim Tivoli Service Request Manager Start Center an.
2. Klicken Sie auf **Go to** > **Assets** > **Resourcs (IntOpCtr)** (Weiter mit > Assets > Ressourcen (IntOpCtr)).
3. Klicken Sie im Fenster **IOC Resources** (IOC-Ressourcen) auf das Symbol **New Resource** (Neue Ressource).
4. Geben Sie auf der Registerkarte **Resource** die folgenden Details ein:

   Ressource
   Eine eindeutige ID für die Ressource.

   Langbeschreibung
   Der Name der Ressource, der in der IBM Intelligent Operations Center-Benutzerschnittstelle im Portlet "Details" auf der Registerkarte "**Ressourcen**" angezeigt wird.

   Kurzbeschreibung
   Eine Kurzbeschreibung der Ressource, die als Direkthilfe angezeigt wird, wenn Sie den Mauszeiger über die Ressource im Portlet "Karte" in der IBM Intelligent Operations Center-Benutzerschnittstelle bewegen.

   Breitengrad
   Der Breitengrad des Standorts der Ressource.

   Längengrad
   Der Längengrad des Standorts der Ressource.
5. Klicken Sie auf die Registerkarte **Capabilities** (Funktionen).
6. Klicken Sie neben dem Feld **Klassification** auf das Symbol **Detail Menu** und anschließend auf **Classify** (Klassifikation > Detailmenü > Klassifizieren).
7. Durchsuchen Sie im Fenster **Classify** (Klassifizieren) die Navigationsstruktur, um die entsprechende Ressourcenklassifikation zu finden.
8. Klicken Sie auf einen Klassifikationsnamen, z. B. ein Warehouse. Eine Tabelle mit den Funktionen, die der Klassifikation zugeordnet sind, wird im Fenster **IOC Resources** (IOC-Ressourcen) angezeigt.
9. Klicken Sie in der Tabelle "Capabilities" (Funktionen) auf die entsprechenden Funktionen und geben Sie **Numeric value** (Numerischer Wert) ein.
10. Klicken Sie auf das Symbol **Save Resource** (Ressource speichern).

Nächste Schritte

Prüfen Sie, ob die Ressource in den folgenden IBM Intelligent Operations Center-Datenbanktabellen aufgelistet ist:

- `IOC.RESOURCE`
- `IOC.RESOURCE_X_CAPABILITY`

Zugehörige Tasks:

„Ereigniskategorie/Funktion-Zuordnung erstellen oder ändern” auf Seite 141

Ressourcen werden im Portlet "Karte" in Abhängigkeit von der Kategorie des ausgewählten Ereignisses und von den zugeordneten Ressourcenfunktionen angezeigt. Bevor Sie eine Ressource erstellen, ordnen Sie die Funktion der Ressource der entsprechenden Ereigniskategorie zu.

Ressource anzeigen, aktualisieren oder löschen

Greifen Sie auf die Tivoli Service Request Manager-Benutzerschnittstelle über die IBM Intelligent Operations Center-Benutzerschnittstelle zu, um Ihre Ressourcen anzuzeigen, zu aktualisieren oder zu löschen.

Informationen zu diesem Vorgang

Das folgende Verfahren beschreibt, wie Sie auf Ressourcendaten in Tivoli Service Request Manager über die IBM Intelligent Operations Center-Benutzerschnittstelle zugreifen. Führen Sie die folgenden Schritte aus, um auf Ressourcendaten direkt über Tivoli Service Request Manager zuzugreifen:

1. Melden Sie sich bei der Tivoli Service Request Manager Start Center an.
2. Klicken Sie auf **Go to** > **Assets** > **Resources (IntOpCtr)** (Weiter mit > Assets > Ressourcen (IntOpCtr)).
3. Um alle IBM Intelligent Operations Center-Ressourcen aufzulisten, klicken Sie im Fenster **Resources (IntOpCtr)** auf der Registerkarte **List** in das Feld **Resource** und drücken Sie die Eingabetaste.
4. Klicken Sie in der Liste auf die Zeile für die Ressource, die Sie ändern möchten.
5. Klicken Sie auf die Registerkarte **Resource** oder ggf. auf die Registerkarte **Capabilities** (Funktionen).

Vorgehensweise

1. Öffnen Sie die IBM Intelligent Operations Center-Benutzerschnittstelle.
2. Bestimmen Sie im Portlet "Details" auf der Registerkarte **Ereignisse und Vorfälle** ein Ereignis in der Liste, dessen Ressourcen Sie anzeigen, aktualisieren oder löschen möchten.
3. Soll eine Liste der Ressourcen im näheren Umfeld des Ereignisses angezeigt werden, klicken Sie mit der rechten Maustaste auf **Ressourcen in der Nähe anzeigen** und wählen Sie den Radius des gewünschten Bereichs aus. Auf der Registerkarte **Ressourcen** wird eine Liste mit Ressourcen angezeigt.
4. Klicken Sie auf der Registerkarte **Ressourcen** mit der rechten Maustaste auf eine Zeile in der Ressourcenliste und wählen Sie in dem angezeigten Menü die gewünschte Option aus:
   - Sollen die Informationen zu einer Ressource aktualisiert werden, klicken Sie auf **Aktualisieren**.
   - Soll eine Ressource aus der Liste und aus der Karte entfernt werden, klicken Sie auf **Löschen**.
   - Sollen Informationen zu einer Ressource angezeigt werden, klicken Sie auf **Eigenschaften**.

   Die Ressource wird (unabhängig von der von Ihnen gewählten Option) in Tivoli Service Request Manager auf der Registerkarte **Ressource** angezeigt.
5. Sie können in Tivoli Service Request Manager auf der Registerkarte **Ressource** die folgenden Aktionen für die Ressource ausführen:
   - Den Ressourcennamen, Beschreibungen, Breitengrad und Längengrad aktualisieren.
   - Um die Ressource zu löschen, wählen Sie **Ressource löschen** aus der Liste **Aktion auswählen** aus.
6. Sie können auf der Registerkarte **Funktionen** die folgenden Aktionen für die Ressourcenfunktionen ausführen.
   - Klicken Sie auf die entsprechenden Funktionen und ändern Sie den Wert unter **Numeric Value**. Damit eine Funktion der Ressource zugeordnet wird, muss der Wert 1 oder höher sein.
   - Wählen Sie eine Funktion aus und klicken Sie anschließend auf das Symbol **Mark Row for Delete** (Zeile zum Löschen markieren) am Ende der Zeile.
7. Wenn Sie mit der Aktualisierung der Ressource fertig sind, klicken Sie auf das Symbol **Save Resource** (Ressource speichern).

Nächste Schritte

Um die aktualisierten Ressourcendaten in der IBM Intelligent Operations Center-Benutzerschnittstelle anzeigen zu können, müssen Sie die Karte zurücksetzen. Prüfen Sie anschließend die Ressourcen für ein Ereignis im Portlet "Details".

Ressourcentyp erstellen

Ressourcentyp in in Tivoli Service Request Manager erstellen.

Informationen zu diesem Vorgang

Sie können eine Hierarchie mit Ressourcentypen definieren, sodass Ressourcentypen über untergeordnete Ressourcen verfügen usw.

Vorgehensweise

1. Melden Sie sich als Administrator beim Tivoli Service Request Manager Start Center an.
2. Klicken Sie auf **Go to** > **Administration** > **Classifications** (Weiter mit > Administration > Klassifikationen).
3. Um alle bestehenden IBM Intelligent Operations Center-Ressourcentypen anzuzeigen, geben Sie auf der Registerkarte **List** im Feld **Description** (Beschreibung) `RESOURCE` ein. Alle Ressourcentypen in der Hierarchie werden angezeigt.
4. Klicken Sie auf den Ressourcentyp oder auf den untergeordneten Ressourcentyp, für den Sie einen untergeordneten Ressourcentyp erstellen möchten. Die Klassifikationsdetails für das übergeordnete Element des neuen Ressourcentyps werden auf der Registerkarte **Classifications** (Klassifikationen) angezeigt.
5. Klicken Sie auf der Registerkarte **Classifications** (Klassifikationen) unter "Children" (Untergeordnete Elemente) auf **New Row** (Neue Zeile).
6. Geben Sie in der leeren Zeile, die der Liste angehängt wird, die folgenden Werte für den neuen Ressourcentyp ein:
   a. Geben Sie in der Spalte **Classification** (Klassifikation) einen Namen ein.
   b. Geben Sie in der Spalte "Classification Desc" (Klassifikationsbeschreibung) eine Beschreibung ein.
   c. Um zu verhindern, dass ein Ressourcentypname beim Speichern des Ressourcentyps geändert wird, heben Sie die Auswahl des Kontrollkästchens **Generate Description** (Beschreibung generieren) auf.
7. Klicken Sie auf das Symbol **Save Classification** (Klassifikation speichern).
8. Führen Sie folgende Unterschritte aus, um ein grafisches Symbol für den neuen Ressourcentyp hinzuzufügen:
   a. Speichern Sie Kopien der Grafik in zwei Größen im PNG-Format. Das größere grafische Symbol wird im Portlet "Karte" angezeigt und das kleinere grafische Symbol wird in der Ereignisliste im Portlet "Details" angezeigt.

      Größe 24 Pixel x 24 Pixel
      Beispiel: *Neue_Ressource*_24.png

      Größe 16 Pixel x 16 Pixel
      Beispiel: *Neue_Ressource*_16.png
   b. Kopieren Sie jede PNG-Datei in das entsprechende Verzeichnis auf dem Anwendungsserver:
      - `/opt/IBM/WebSphere/wp_profile/installedApps/ICPWPSNode/iss_portal_ear.ear/iss_common_widgets_web.war/images/resource_icons/PNG-24x24/Normal_State`
      - `/opt/IBM/WebSphere/wp_profile/installedApps/ICPWPSNode/iss_portal_ear.ear/iss_common_widgets_web.war/images/resource_icons/PNG-16x16/Normal_State`
   c. Stellen Sie sicher, dass jedes Symbol im entsprechenden Web-Browser-Link korrekt angezeigt wird:

- http://**appserver**/ibm/iss/common/widgets/images/resource_icons/PNG-24x24/Normal_State/new_resource_24.png
- http://**appserver**/ibm/iss/common/widgets/images/resource_icons/PNG-16x16/Normal_State/new_resource_16.png

Funktion einem Ressourcentyp hinzufügen

Erstellen Sie eine Funktion in Tivoli Service Request Manager.

Vorgehensweise

1. Melden Sie sich als Administrator beim Tivoli Service Request Manager Start Center an.
2. Klicken Sie auf **Go to** > **Administration** > **Classifications** (Weiter mit > Administration > Klassifikationen).
3. Um alle bestehenden IBM Intelligent Operations Center-Ressourcenklassifikationen anzuzeigen, filtern Sie auf der Registerkarte **List** nach `RESOURCE`.
4. Klicken Sie auf die Registerkarte **Classifications** (Klassifikationen).
5. Klicken Sie unter "Children" (Untergeordnete Elemente) in der Liste auf den Ressourcentyp, für den Sie eine Funktion hinzufügen möchten.
6. Um zu verhindern, dass ein Ressourcenname beim Speichern der Klassifikation geändert wird, heben Sie die Auswahl des Kontrollkästchens **Generate Description** (Beschreibung generieren) auf.
7. Klicken Sie unter "Attributes" (Attribute) auf **New Row** (Neue Zeile).
8. Geben Sie die Details für die neue Funktion ein:
   a. Geben Sie für **Attribut** einen Namen ein.
   b. Geben Sie im Feld rechts vom Feld **Attribut** eine Beschreibung ein.
   c. Um einen Wert für **Data Type** (Datentyp) einzugeben, klicken Sie auf das Symbol "Select Value" (Wert auswählen) und wählen Sie einen Wert im Fenster **Select Value** (Wert auswählen) aus.
   d. Um anzugeben, dass für untergeordnete Ressourcen diese Funktion übernommen wird, wählen Sie **Apply Down Hierarchy?** (Abwärtshierarchie anwenden) aus.
9. Klicken Sie auf das Symbol **Save Classification** (Klassifikation speichern).

Beispiele für Standard Operating Procedures, Workflows und Ressourcen

Beispiele für Standard Operating Procedures, Workflows und Ressourcen werden bereitgestellt, wenn Sie IBM Intelligent Operations Center Version 1.5 installieren.

Standard Operating Procedures

Die folgenden drei Standard Operating Procedures werden bereitgestellt:

PLUSIMITIG: Anfangsvorbereitung für Unwetter (Milderung)
PLUSIMITIG enthält die folgenden Schritte:

1. Den Schweregrad des Wetters prüfen. Manueller Schritt ohne zugeordnete Workflows.
2. Bei Bedarf Sicherheitseinstufung erhöhen. Manueller Schritt ohne zugeordnete Workflows.

PLUSIPREPA: Vorbereitung für Evakuierung aufgrund von Unwetter (Vorbereitung)
PLUSIPREPA enthält die folgenden Schritte:

1. Notunterkünfte vorbereiten. Manueller Schritt mit zugeordnetem Workflow PLUSISOP00.
2. Unterstützungsressourcen für Evakuierung bestimmen. Manueller Schritt mit zugeordnetem Workflow PLUSISOP00.

3. Verfügbarkeit von Unterstützungsressourcen bewerten. Manueller Schritt mit zugeordnetem Workflow PLUSISOP00.

PLUSIRESPO: Evakuierung betroffener Bereiche (Reaktion und Rettung)
PLUSIRESPO enthält die folgenden Schritte:

1. Evakuierungsanweisung genehmigen. Manueller Schritt ohne zugeordnete Workflows.
2. Sicherstellen, dass die Fluchtwege frei sind. Manueller Schritt ohne zugeordnete Workflows.

Die Auswahlmatrix für Standard Operating Procedure wird mit Daten aufgefüllt, die die Auswahl der drei Standard Operating Procedures auslösen, wie in der folgenden Tabelle veranschaulicht:

Tabelle 35. Auswahlmatrix für Standard Operating Procedure-Beispieldaten

Kategorie	Schweregrad	Dringlichkeit	Gewissheit	Standard Operating Procedure-Name
Met	Schwerwiegend	In der Zukunft	Beobachtet	PLUSIMITIG
Met	Schwerwiegend	In der Zukunft	Wahrscheinlich	PLUSIMITIG
Met	Extrem	In der Zukunft	Beobachtet	PLUSIPREPA
Met	Extrem	In der Zukunft	Wahrscheinlich	PLUSIPREPA
Met	Extrem	Sofort	Beobachtet	PLUSIRESPO

BeispielWorkflow

Es gibt einen BeispielWorkflow:

PLUSISOP00: Die Aktivitätsaktion abschließen
Der PLUSISOP00-Workflow löst eine Aktion aus, um den Status einer Aktivität in `COMP` (abgeschlossen) zu ändern.

Der Workflow PLUSISOP00 ist jedem Schritt in der Beispiel-Standard Operating Procedure PLUSIPREPA zugeordnet. Wenn Sie einen der Schritte starten, wird der Status des Schritts automatisch als abgeschlossen markiert.

Beispielressourcen

In der folgenden Tabelle sind die Beispielressourcen aufgelistet, die in der Domäne `PLUSICATCPLMAP` bereitgestellt werden:

Tabelle 36. Beispielressourcen

Ressource	Beschreibung	Ressourcentyp
BASCOMEYE	Bascombe Eye Institute	RESOURCES\HOSPITAL
BLUEFISHW	Blue Fish Warehouse	RESOURCES\WAREHOUSE
DOCTORSH	Doctor's Hospital	RESOURCES\HOSPITAL
MERYCYH	Mercy Hospital	RESOURCES\HOSPITAL
MAMICHILD	Miami Children's Hospital	RESOURCES\HOSPITAL
SFFOODDIST	South Florida Food Distribution	RESOURCES\WAREHOUSE
TTLEASING	Tropical Trailer Leasing Corporation	RESOURCES\WAREHOUSE
UNIMIAMI	University of Miami Hospital	RESOURCES\HOSPITAL
WTDCDIST	WTDC Distribution Center Miami	RESOURCES\WAREHOUSE

Kapitel 5. Anpassung der Lösung

Zum Anpassen der Lösung an Ihre speziellen Anforderungen müssen die in diesem Abschnitt aufgeführten Tasks in Bezug auf die Benutzerschnittstelle und die Systemeigenschaftentabelle ausgeführt werden. Die Anpassung steht in enger Beziehung mit der Integration der Lösung und die entsprechenden Links sind in den Themen zum Ereignis und zum KPI (Key Performance Indicator) in diesem Abschnitt enthalten.

Benutzerschnittstelle anpassen

Sie können Elemente der Benutzerschnittstelle des IBM Intelligent Operations Center anpassen, um sie an Ihre Anforderungen anzupassen.

Zusätzlich zur Anpassung des Layouts und der Darstellung von Portlets können Sie auch neue Seiten erstellen. Weitere Information finden Sie in der Produktdokumentation zu WebSphere Portal.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Benutzerschnittstelle lokalisieren

Die Browsereinstellungen bestimmen die Einstellungen für Sprache, Datum und Uhrzeit für die Benutzerschnittstelle des IBM Intelligent Operations Center. Ein Administrator kann die Formate für Datum und Uhrzeit anpassen.

Im IBM Intelligent Operations Center bestimmen Ihre Browsereinstellungen die Sprache des Texts. Wenn diese Sprache im IBM Intelligent Operations Center nicht verfügbar ist, wird die möglichst nahe verwandte Sprache verwendet. So wird z. B. bei kanadischem Französisch auf Französisch (Frankreich) zurückgegriffen und von diesem wiederum auf Englisch, was immer verfügbar ist. Ihre Browsereinstellungen bestimmen außerdem die Zeitzone für alle Datums- und Uhrzeitanzeigen. Datum und Uhrzeit werden im IBM Intelligent Operations Center automatisch an die Zeitzone des Browsers angepasst.

Alle Datums- und Zeitangaben werden in Ihrer Zeitzone in dem Format angezeigt, das in der Datenbanktabelle mit den Systemeigenschaften festgelegt ist. Systemeigenschaften enthalten die Zeichenfolgen des Datums- und Uhrzeitformats. Zur Änderung des Wertes in der Datenbank durch Bearbeiten der Eigenschaft folgen Sie dem Link am Ende dieses Themas.

Zugehörige Konzepte:

„Systemweite Konfigurationsdaten angeben" auf Seite 188
In der Tabelle mit den Systemeigenschaften von IBM Intelligent Operations Center sind IBM Intelligent Operations Center-Konfigurationsdaten gespeichert.

„CAP für KPI-Ereignisse verwenden" auf Seite 103
Der WebSphere Message Broker, der als Teil vom IBM Intelligent Operations Center bereitgestellt wird, akzeptiert CAP-Ereignisnachrichten und verwendet die Dateien in KPI-Berechnungen (Key Performance Indicator).

Liste der Portlets

IBM Intelligent Operations Center ist eine portletbasierte Lösung, die Portaltechnologie verwendet, um Tools bereitzustellen und Informationen anzuzeigen. Alle in IBM Intelligent Operations Center enthaltenen Portlets sind in den folgenden Abschnitten aufgelistet.

Benutzerportlets

In der folgenden Tabelle sind die Benutzerportlets aufgelistet, die im IBM Intelligent Operations Center enthalten sind. In der Tabelle sind auch die Beispielseitenansichten angegeben, in denen die jeweiligen Portlets verfügbar sind.

Sie können die Portlets anpassen. Weitere Informationen erhalten Sie über den Link am Ende des Themas.

Tabelle 37. Benutzerportlets im IBM Intelligent Operations Center

Portlet	Beschreibung	Beispielseitenansichten
„Kontakt” auf Seite 286	Im Portlet "Kontakt" können Ihre Kontakte (Ansprechpartner) nach bestimmten Kategorien angezeigt werden. Sie können die Anordnung nach Personen vornehmen, mit denen Sie kommunizieren müssen. Sie können beispielsweise eine Kategorie für allgemeine Tätigkeiten und eine weitere Kategorie für projektspezifische Tätigkeiten besitzen. Mit dem Portlet "Kontakt" können Sie mit Personen kommunizieren sowie Ihren Onlinestatus, Ihre Ansprechpartner oder Gruppen ändern.	• „Ansicht "Aufsichtsperson: Status"” auf Seite 281 • „Ansicht "Aufsichtsperson: Vorgänge"” auf Seite 282 • „Ansicht "Betreiber: Vorgänge"” auf Seite 283
„Details” auf Seite 287	"Details" ist ein interaktives Listenportlet. Alle Ereignisse, zu deren Anzeige Sie berechtigt sind, sind in der Ereignisliste sowie in allen Kartenportlets enthalten, die mit dem Portlet "Details" verknüpft sind.	• „Ansicht "Aufsichtsperson: Vorgänge"” auf Seite 282 • „Ansicht "Betreiber: Vorgänge"” auf Seite 283 • „Ansicht "Positionskarte"” auf Seite 285
„Key Performance Indicator - Drilldown” auf Seite 290	Soll eine bestimmte KPI-Kategorie im Portlet "Key Performance Indicator - Drilldown" näher betrachtet werden, klicken Sie im Portlet "Status" auf die Kategorie. Die Kategorie wird daraufhin im Portlet "Key Performance Indicator - Drilldown" angezeigt. In der Liste können Sie die untergeordneten KPIs überprüfen, bis Sie zu den Details des KPI gelangen, der die Statusänderung bewirkt hat.	• „Ansicht "Aufsichtsperson: Status"” auf Seite 281
„Positionskarte” auf Seite 291	Mit dem Portlet "Positionskarte" können Sie die auf einer Positionskarte markierten Ereignisse anzeigen. Eine Positionskarte im IBM Intelligent Operations Center ist eine Karte oder ein Plan mit vordefinierten Interaktionsbereichen, wie z. B. Sitzbereiche in großen Sportstadien.	• „Ansicht "Positionskarte"” auf Seite 285

Tabelle 37. Benutzerportlets im IBM Intelligent Operations Center (Forts.)

Portlet	Beschreibung	Beispielseitenansichten
„Karte" auf Seite 294	Im Portlet "Karte": Eine Karte der geografischen Region mit Ereignis- und Ressourcenmarkierungen. Ein Filterformular für die Auswahl der Ereigniskategorien, die in der Karte und in den mit dem Portlet "Karte" verknüpften Portlets angezeigt werden sollen. Ein Filterformular für die Auswahl der Funktionen der Ressourcen, die auf der Karte und auf der Registerkarte **Ressourcen** im verknüpften Portlet "Details" angezeigt werden sollen. Um dieses Formular anzuzeigen, wählen Sie zunächst im Portlet "Details" die Option **Ressourcen in der Nähe anzeigen** aus.	• „Ansicht "Aufsichtsperson: Vorgänge"" auf Seite 282 • „Ansicht "Betreiber: Vorgänge"" auf Seite 283
„Meine Aktivitäten" auf Seite 300	Angemeldete Benutzer können die ihnen zugeordneten Aktivitäten im Portlet "Meine Aktivitäten" anzeigen. Im Portlet "Meine Aktivitäten" sind die Aktivitäten nach übergeordneten SOPs (Standard Operating Procedures) angeordnet. Jede Standard Operating Procedure entspricht einem Ereignis.	• „Ansicht "Aufsichtsperson: Status"" auf Seite 281 • „Ansicht "Aufsichtsperson: Vorgänge"" auf Seite 282 • „Ansicht "Betreiber: Vorgänge"" auf Seite 283
„Benachrichtigungen" auf Seite 302	Das Portlet "Benachrichtigungen" stellt eine dynamische, interaktive Liste der Alerts bereit, die aufgrund geänderter KPI-Werte und damit in Zusammenhang stehender Ereignisse ausgegeben werden. Dieses Portlet hat die Aufgabe, auf Änderungen von KPI-Werten oder des Ereignisstatus hinzuweisen. Die Liste enthält wichtige Angaben zu jedem Alert.	• „Ansicht "Aufsichtsperson: Status"" auf Seite 281 • „Ansicht "Aufsichtsperson: Vorgänge"" auf Seite 282 • „Ansicht "Betreiber: Vorgänge"" auf Seite 283
„Berichte" auf Seite 304	Mit dem Portlet "Berichte" können Berichte von Ereignissen in Form von Diagrammen angezeigt werden. In diesem Portlet gibt es mehrere Möglichkeiten für die Anordnung von Ereignissen; darüber hinaus können Ereignisse nach einem bestimmten Datum oder Zeitraum ausgewählt werden. Mithilfe dieser Berichte können Sie Maßnahmen für aktuelle und künftige Ereignisse planen.	• „Aufsichtsperson: Berichte" auf Seite 284 • „Betreiber: Berichte" auf Seite 284

Tabelle 37. Benutzerportlets im IBM Intelligent Operations Center (Forts.)

Portlet	Beschreibung	Beispielseitenansichten
„Status" auf Seite 306	Das Portlet "Status" stellt eine für Entscheidungsträger hilfreiche Statusübersicht der KPIs aller Einrichtungen bereit, für die eine Anzeigeberechtigung erteilt wurde. In diesem Portlet können Sie aktuelle Änderungen am KPI-Status anzeigen und damit planen und bei Bedarf entsprechende Maßnahmen vornehmen.	• „Ansicht "Aufsichtsperson: Status"" auf Seite 281

Zugehörige Tasks:

„Portlets anpassen" auf Seite 154
Als Administrator können Sie die Portleteinstellungen ändern, um ein Portlet anzupassen.

Verwaltungsportlets

In der folgenden Tabelle sind die Verwaltungsportlets aufgelistet, die im IBM Intelligent Operations Center enthalten sind. Die Verwaltungsportlets befinden Sie sich auf der Verwaltungsseite.

Tabelle 38. Verwaltungsportlets im IBM Intelligent Operations Center

Portlet	Beschreibung
„Produktinformationen" auf Seite 205	Im Portlet "Produktinformationen" können Sie Details zur Version des IBM Intelligent Operations Center und zur Version der integrierten IBM Smarter Cities Software Solutions anzeigen, die Sie installiert haben. Außerdem können Sie Details zu allen Aktualisierungen anzeigen, die Sie seit der Installation ausgeführt haben.
„Administrationskonsolen" auf Seite 213	Mit dem Portlet "Administrationskonsolen" können Sie die Services verwalten, die von der Lösung bereitgestellt werden.
„Komponenten überprüfen" auf Seite 220	Mit dem Systemprüfungstool wird überprüft, ob auf die Komponenten in IBM Intelligent Operations Center zugegriffen werden kann und ob sie betriebsbereit sind.
„Zusammenfassung der Benutzerberechtigungen" auf Seite 86	Im Portlet "Zusammenfassung der Benutzerberechtigungen" werden Details zur Gruppenzugehörigkeit und zu den erteilten Benutzerberechtigungen angezeigt.
„Key Performance Indicators (KPIs)" auf Seite 178	Im Portlet "Key Performance Indicators (KPIs)" können Sie KPIs anzeigen, ändern, kopieren, erstellen und löschen. Darüber hinaus können Sie die in den Portlets "Status" und "Key Performance Indicator - Drilldown" angezeigten KPI-Hierarchien anpassen.
„Positionskartenmanager" auf Seite 186	Mithilfe des Portlets "Positionskartenmanager" können Sie das Portlet "Positionskarte" anpassen.
„Standard Operating Procedures" auf Seite 135	Für die Verwaltung von Ereignissen, die im IBM Intelligent Operations Center auftreten, können Sie Standard Operating Procedures und Aktivitäten definieren. Verwenden Sie das Portlet "Standard Operating Procedures", um auf Standard Operating Procedure, Auswahlmatrix für Standard Operating Procedure und Workflow-Designer-Anwendungen in Tivoli Service Request Manager zuzugreifen.

Tabelle 38. Verwaltungsportlets im IBM Intelligent Operations Center (Forts.)

Portlet	Beschreibung
„Erstellung von Ereignisscripts" auf Seite 114	Mit dem Portlet "Erstellung von Ereignisscripts" können Sie ein Script zum Erstellen einer sequenziellen Liste von Ereignissen schreiben, die nacheinander in vorgegebenen Zeitintervallen veröffentlicht werden sollen.
„Beispiel-Publisher" auf Seite 110	Das Portlet "Beispiel-Publisher" ist ein Tool für automatisierte Tests, mit dem Administratoren die Lösung verwalten und überprüfen können. So können Administratoren mit dem Portlet "Beispiel-Publisher" als Clientanwendung die Veröffentlichung von CAP-Nachrichten in IBM Intelligent Operations Center testen. Damit entfällt bei Verwendung des Portlets "Beispiel-Publisher" die Notwendigkeit, Testclientanwendungen manuell zu erstellen.

Zugehörige Tasks:

„Portlets anpassen" auf Seite 154
Als Administrator können Sie die Portleteinstellungen ändern, um ein Portlet anzupassen.

Seite erstellen oder anpassen

Sie können neue Seiten erstellen, die im IBM Intelligent Operations Center einbezogen werden sollen, und angeben, welche Portlets auf diesen Seiten angezeigt werden. Sie können die Anzeigengestaltung und das Layout der Portlets auf jeder Seite anpassen.

Informationen zu diesem Vorgang

Verwenden Sie die WebSphere Portal-Benutzerschnittstelle, um Seiten und Portlets anzupassen.

Anmerkung: Wenn Sie ein Seitenlayout erstellen oder bearbeiten, stellen Sie sicher, dass die Portlets ordnungsgemäß funktionieren, indem die folgenden Regeln eingehalten werden:

- Die Portlets "Karte" und "Details" müssen sich in derselben Gruppe und auf derselben Seite befinden, damit ein Ereignis vom Portlet "Karte" hinzugefügt werden kann.
- Die Portlets "Meine Aktivitäten" und "Details" müssen sich in derselben Gruppe und auf derselben Seite befinden, damit Ereignisdetails vom Portlet "Meine Aktivitäten" oder SOP-Details vom Portlet "Details" angefordert werden können.

Vorgehensweise

1. Zum Öffnen von WebSphere Portal klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie in WebSphere Portal auf **Portalbenutzerschnittstelle**.
3. Klicken Sie auf die gewünschte Option:
   - Zum Arbeiten mit Ihren Seiten oder zur Erstellung neuer Seiten klicken Sie auf **Seiten verwalten**.
   - Zum Eintragen von Motiven und Skins stellen Sie das Standardmotiv sowie die Standardskin für jedes Motiv ein und klicken Sie auf **Motive und Skins**.
   - Zum Anpassen der wichtigsten Siteelemente in Motiven, einschließlich Titel, Navigation, Schriftart und Farben, klicken Sie auf **Motivanpassung**.
4. Führen Sie die gewünschten Änderungen durch. Weitere Informationen zur Verwendung von WebSphere Portal zur Anpassung von Portlets finden Sie unter dem Link am Ende des Themas zur WebSphere Portal-Produktdokumentation.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Portlets anpassen

Als Administrator können Sie die Portleteinstellungen ändern, um ein Portlet anzupassen.

Informationen zu diesem Vorgang

Sie haben zwei Möglichkeiten zur Anpassung; bei beiden Methoden werden die Portleteinstellungen für alle Benutzer geändert:

- **Edit Shared Settings** (Gemeinsam genutzte Einstellungen bearbeiten): Über diese Option werden nur die Einstellungen für die aktuelle Portletinstanz geändert.
- **Configure** (Konfigurieren): Über diese Option werden die globalen Portleteinstellungen für alle vorhandenen Portletinstanzen geändert.

Welche Anpassungsmöglichkeiten Sie haben, hängt von den Berechtigungen ab, die Ihrer Benutzer-ID zugeordnet sind. Globale Einstellungen werden durch gemeinsam genutzte Einstellungen außer Kraft gesetzt.

Vorgehensweise

1. Melden Sie sich beim Lösungsportal als Administrator an.
2. Klicken Sie in die rechte obere Ecke des Portlets, um das Portletmenü anzuzeigen.
3. Klicken Sie auf **Gemeinsam genutzte Einstellungen bearbeiten** oder auf **Konfigurieren**.
4. Geben Sie Ihre Einstellungen in die bereitgestellten Felder ein.
5. Um das Fenster für Einstellungen zu schließen, klicken Sie auf eine der folgenden Schaltflächen:
   - **Speichern**, um die Änderungen zu speichern.
   - **Abbrechen**, um den Änderungsvorgang abzubrechen.
   - **Auf Standardeinstellungen zurücksetzen**, um wieder die globalen Standardeinstellungen zu verwenden.

Ergebnisse

Die von Ihnen gespeicherten, neuen Einstellungen werden nach der nächsten Aktualisierung des Portlets wirksam. Die mit dem IBM Intelligent Operations Center bereitgestellten Standardwerte für globale Einstellungen werden für alle Parameter verwendet, die nicht neu eingestellt wurden.

Einstellungen des Produktinformationen-Portlets

Anpassen des Produktinformationen-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Produktinformationen-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 39. Anpassungsparameter des Produktinformationen-Portlets

Parameter	Beschreibung	Standardwert
Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	400
Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	600

Zugehörige Konzepte:

„Produktinformationen” auf Seite 205
Im Portlet "Produktinformationen" können Sie Details zur Version des IBM Intelligent Operations Center und zur Version der integrierten IBM Smarter Cities Software Solutions anzeigen, die Sie installiert haben. Außerdem können Sie Details zu allen Aktualisierungen anzeigen, die Sie seit der Installation ausgeführt haben.

Einstellungen des Administrationskonsolen-Portlet

Anpassen des Administrationskonsolen-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Administrationskonsolen-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 40. Anpassungsparameter des Administrationskonsolen-Portlet

Parameter	Beschreibung	Standardwert
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`AdministrationConsolePortletHelp`
Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	`400`
Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	`450`
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der von der Lösung bereitgestellte Titel angezeigt. Dieser lautet Administrationskonsolen.
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.

Zugehörige Konzepte:

„Administrationskonsolen” auf Seite 213
Mit dem Portlet "Administrationskonsolen" können Sie die Services verwalten, die von der Lösung bereitgestellt werden.

Einstellungen des Kontakt-Portlets

Anpassen des Kontakt-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Kontakt-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 41. Anpassungsparameter des Kontakt-Portlets

Parameter	Beschreibung	Standardwert
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`SametimeWebClientPortletHelp`
Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	`250`
Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	`600`
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der folgende von der Lösung bereitgestellte Titel angezeigt: Kontakt.
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.

Zugehörige Konzepte:

„Kontakt" auf Seite 286
Mithilfe des Portlets "Kontakt" können Sie Sofortnachrichten innerhalb der Lösung senden.

Einstellungen des Details-Portlets

Anpassen des Details-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Details-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 42. Anpassungsparameter des Details-Portlets

Parametername	Beschreibung	Standardwert
Columns (Spalten)	Spezifikationen und die Reihenfolge der Spalten, die in der Liste angezeigt werden sollen.	`[{"id": "commonevents.headline", "width": "20"}, {"id": "commonevents.eventType", "width": "7"}, {"id": "commonevents.category", "width": "10"}, {"id": "commonevents.severity", "width": "10"}, {"id": "commonevents.certainty", "width": "10"}, {"id": "commonevents.urgency", "width": "10"}, {"id": "commonevents.sent", "width": "12", "sortPriority": "1", "sortAscending": "false"}]`

Tabelle 42. Anpassungsparameter des Details-Portlets (Forts.)

Bedingungen	Zusätzliche Bedingungen für die Anzeige von Ereignissen oder Ressourcen. Zusätzliche Bedingungen können nicht mithilfe der Symbolleiste oder des Kartenfilters außer Kraft gesetzt werden. Entsprechend der Standardeinstellung werden keine zusätzlichen Bedingungen angewendet.	`[]`
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`CommonEventsPortletHelp`
Hinzugefügtes Ereignis ausblenden	Einstellung des Typs "true" (Wahr) oder "false" (Falsch), um die Schaltfläche **Ereignisse hinzufügen** und die Popup-Menü-Option aus- oder einzublenden.	`true`
Hinzugefügte Ressource ausblenden	Einstellung des Typs "true" (Wahr) oder "false" (Falsch), um die Schaltfläche **Ressourcen hinzufügen** in der Registerkarte **Ressourcen** aus- oder einzublenden.	`true`
Ereignisse ausblenden	Einstellung des Typs "true" (Wahr) oder "false" (Falsch), um die Registerkarte **Ereignisse und Vorfälle** aus- oder einzublenden.	`false`
Ressourcen ausblenden	Einstellung des Typs "true" (Wahr) oder "false" (Falsch), um die Registerkarte **Ressourcen** aus- oder einzublenden.	`false`
Symbolleiste ausblenden	Einstellung des Typs "true" (Wahr) oder "false" (Falsch), um die Symbolleiste am Anfang der Liste aus- oder einzublenden.	`true`
Ressourcenabbruchmodus ignorieren	Einstellung des Typs "true" (Wahr) oder "false" (Falsch), um eine vom Karte-Portlet eingehende Nachricht zum Ressourcenabbruchmodus zu bestätigen oder zu ignorieren.	`false`
Ereigniserstellung ignorieren	Einstellung von "true" (Wahr) oder "false" (Falsch), um Ereignisse zu bestätigen oder zu ignorieren, die vom Benutzer im Karte-Portlet erstellt wurden.	`false`
Ereignisfilteränderungen ignorieren	Einstellung von "true" (Wahr) oder "false" (Falsch), um die Auswahl von Ereignisfiltern zu bestätigen oder zu ignorieren, die vom Benutzer im Karte-Portlet getroffen wurde.	`false`
Ereignisauswahl ignorieren	Einstellung von "true" (Wahr) oder "false" (Falsch), um die Auswahl eingehender Ereignisse zu bestätigen oder zu ignorieren, die vom Benutzer im Karte-Portlet getroffen wurde.	`false`

Tabelle 42. Anpassungsparameter des Details-Portlets (Forts.)

Ereignistasks ignorieren	Einstellung von "true" (Wahr) oder "false" (Falsch), um alle Auswahlmöglichkeiten im Popup-Menü eines Ereignisses zu bestätigen oder zu ignorieren.	`false`
Zurücksetzung einer Karte ignorieren	Einstellung des Typs "true" (Wahr) oder "false" (Falsch), um einen Klick auf die Schaltfläche **Ressourcen** zu bestätigen oder zu ignorieren.	`false`
Ressourcenfilteränderung ignorieren	Einstellung von "true" (Wahr) oder "false" (Falsch), um die Auswahl von Ressourcenfiltern zu bestätigen oder zu ignorieren, die vom Benutzer im Karte-Portlet getroffen wurde.	`false`
Ressourcentasks ignorieren	Einstellung von "true" (Wahr) oder "false" (Falsch), um alle Auswahlmöglichkeiten im Kontextmenü einer Ressource zu bestätigen oder zu ignorieren.	`false`
Portlet group identifier (Portletgruppen-ID)	Name der Gruppe, der dieses Portlet angehört. Ein allgemeiner Name richtet die Datenübertragung zwischen den Portlets "Karte", "Details" und "Positionskarte" auf derselben Seite ein.	`default`
Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	`350`
Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	`600`
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der folgende von der Lösung bereitgestellte Titel angezeigt: Details.
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.

Anmerkung: Die Erläuterung des Ereignisses für den Portlet-Titel beim Bereitstellen eines Ressourcenpakets gilt gleichermaßen für den Spaltentitel, der aus demselben Ressourcenpaket stammt.

Spaltenparameter (columns)

Der Wert des Parameters **`columns`** (Spalten) ist eine Gruppe von JSON-Objekten, die entsprechend den Erklärungen in Tabelle 43 auf Seite 159 konfiguriert werden können.

Tabelle 43. Objekte innerhalb des Wertes des Spaltenparameters des Details-Portlets

Objekt	Enthält
`id`	die Spalten-ID, um anzuzeigen, dass die Spalte angezeigt werden soll
`width`	Anzahl der Pixel, die die Spaltenbreite angibt.
`format`	Zeichenfolge, die das Format darstellt, das für die Datums- und Uhrzeitspalten zu verwenden ist, wobei der Eintrag die Einstellung in der Tabelle `sysprop` außer Kraft setzt
`sortAscending`	• Der Wert `true`, um eine aufsteigende Sortierreihenfolge für die Spalteneinträge zu verwenden • Der Wert `false`, um eine absteigende Sortierreihenfolge für die Spalteneinträge zu verwenden
`sortPriority`	• Zahl, um die Sortierpriorität dieser Spalte im Vergleich zu allen anderen Spalten anzugeben, wobei die Priorität umso höher ist, je kleiner die Zahl ist • Kein Wert, leer lassen, um die Standardeinstellung der Sortierpriorität der Spalten zu verwenden • Wert `-1`, um die Standardeinstellung der Sortierpriorität der Spalten zu inaktivieren
`title`	Spaltenüberschrift, die nicht zu belegen ist, wenn die Standardüberschrift verwendet werden soll

Spalten werden im Portlet in derselben Reihenfolge angezeigt wie in den JSON-Objekten angegeben, die den Wert des Parameters **`columns`** bilden. Es werden nur die Spalten angezeigt, deren Spalten-ID innerhalb des Wertes liegt. Alle anderen Spalten sind ausgeblendet. Wenn für den Parameters **`columns`** kein Wert angegeben wird, werden die Spalten entsprechend der Standardeinstellung angezeigt, die in der ersten Zeile von Tabelle 42 auf Seite 156 dargestellt ist.

Die gültigen Werte für die Spalten-IDs sind in Tabelle 44 beschrieben.

Tabelle 44. Gültige Spalten-IDs des Details-Portlets

Spalten-ID	Beschreibung
`commonevents.id`	die UUID des Ereignisses in der Tabelle mit allgemeinen Ereignissen
`commonevents.externalEventid`	Vom Sender des Ereignisses zugeordnete Ereignis-ID
`commonevents.specification`	Formatspezifikation, gefolgt von dem Ereignis, z. B. `CAP`
`commonevents.eventType`	Nicht übersetzter Wert für den systemspezifischen Code, der angibt, ob ein Ereignis eskaliert wurde oder nicht: `Ereignis` oder `Vorfall`
`commonevents.sent`	Vom Sender des Ereignisses genannte Sendezeit
`commonevents.headline`	Das Ereignis beschreibende Überschrift
`commonevents.hover text`	Das Ereignis beschreibende Kurzinfo
`commonevents.category`	Nicht übersetzter Kategorienwert
`commonevents.certainty`	Nicht übersetzter Wert für Gewissheit
`commonevents.severity`	Nicht übersetzter Wert für Schweregrad
`commonevents.urgency`	Nicht übersetzter Wert für Dringlichkeit

Tabelle 44. Gültige Spalten-IDs des Details-Portlets (Forts.)

Spalten-ID	Beschreibung
`commonevents.url`	URL-Webadresse für zusätzliche Informationen zu dem Ereignis
`commonevents.externalWorkOrderId`	Zugehörige Auftrags-ID, in der Regel die Tivoli Service Request Manager Standard Operating Procedure-ID
`commonevents.areaId`	Kennung des Positionskartenbereichs, falls das Ereignis mit einer Positionskarte verbunden ist
`commonevents.largeIcon`	Zur Darstellung des Ereignisses auf der Karte verwendetes Symbol
`commonevents.largeHiliteIcon`	Zur Hervorhebung des Ereignisses auf der Karte verwendetes Symbol
`commonevents.largeGreyIcon`	Zur Inaktivierung des Ereignisses auf der Karte verwendetes Symbol
`commonevents.smallIcon`	Für das Ereignis in der Liste verwendetes Symbol
`commonevents.user1`	In der Tivoli Netcool/Impact-Richtlinie festgelegter Wert
`commonevents.user2`	Vom Benutzer in der Tivoli Netcool/Impact-Richtlinie festgelegter Wert
`commonevents.user3`	Vom Benutzer in der Tivoli Netcool/Impact-Richtlinie festgelegter Wert
`commonevents.user4`	Vom Benutzer in der Tivoli Netcool/Impact-Richtlinie festgelegter Wert
`commonevents.user5`	Vom Benutzer in der Tivoli Netcool/Impact-Richtlinie festgelegter Wert

Bedingungsparameter (conditions)

Der Wert des Parameters **`conditions`** (Bedingungen) ist eine Gruppe von JSON-Objekten, die entsprechend den Erklärungen in Tabelle 45 konfiguriert werden können.

Tabelle 45. Objekte innerhalb des Wertes des Bedingungsparameters des Details-Portlets

Objekttyp	Enthält
`selector`	Die Kennung der Spalte, auf die der Operator angewendet wird
`operator`	SQL-Operator, der auf die Werte des Selektors angewendet wird. Folgende Optionen stehen zur Verfügung: • `contains`: wenn die Spalte "selector" den Wert enthält, ist dies die Standardeinstellung • `equals`: wenn die Spalte "selector" dem Wert entspricht • `notEquals`: wenn die Spalte "selector" dem Wert nicht entspricht • `startsWith`: wenn die Spalte "selector" mit dem Wert beginnt • `endsWith`: wenn die Spalte "selector" mit dem Wert endet
`values`	Der Wert der angezeigten Spalte; der Wert muss der nicht übersetzte Schlüsselwert sein wie in der vorangegangenen Tabelle angegeben

Anmerkung:

Der Parameter **conditions** definiert zusätzliche Kriterien zu jenen, die im Filter des Karte-Portlets bereitgestellt werden. Diese Kriterien setzen die im Kartenfilter oder der Symbolleiste festgelegten Bedingungen außer Kraft.

Anmerkung: Die Symbolleiste ist standardmäßig ausgeblendet.

Beispiel: Sie möchten die folgenden Änderungen an Spalten vornehmen:

- Nur die Spalten **Gesendet**, **Überschrift**, **Kategorie** und **URL** anzeigen.
- Die Spaltenbreite für **Gesendet** in `12` ändern.
- Das Spaltenformat für **Gesendet** in `t-MMM-jjjj HH:mm` ändern.
- Die Priorität der Sortierreihenfolge der Spalte **Gesendet** in `2` und der Spalte **Kategorie** in `1` ändern.

Diese Änderungen werden angezeigt, wenn Sie Folgendes in das Feld **Spalten** eingeben und Ihre Benutzervorgaben speichern:

```
[{"id": "commonevents.sent", "width": "10", "format": "d-MMM-yyyy HH:mm", "sortPriority": "2"},
{"id": "commonevents.headline"},  {"id": "commonevents.category", "sortPriority": "1"}, {"id": "commonevents.url"}]
```

Beispiel: Sie möchten nur Ereignisse anzeigen, die die beiden folgenden Bedingungen erfüllen:

- Ein **Schweregrad** von `Extrem` oder `Schwerwiegend`
- Ein **Ereignistyp** `Vorfall`

Diese Änderungen werden angezeigt, wenn Sie Folgendes in das Feld **Bedingungen** eingeben und Ihre Benutzervorgaben speichern:

```
[{"selector": "commonevents.severity", "operator": "equals", "values": ["Extreme", "Severe"]},
{"selector": "commonevents.eventType", "operator": "equals", "values": ["Incident"]}]
```

Zugehörige Konzepte:

„Details" auf Seite 287
Mit dem Portlet "Details" können Sie in IBM Intelligent Operations Center Ereignisse anzeigen, überwachen und verwalten.

Einstellungen des Key Performance Indicator - Drilldown-Portlets

Anpassen des Key Performance Indicator - Drilldown-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Key Performance Indicator - Drilldown-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 46. Anpassungsparameter des Key Performance Indicator - Drilldown-Portlets

Parameter	Beschreibung	Standardwert
Columns (Spalten)	Spezifikationen und die Reihenfolge der Spalten, die in der Liste angezeigt werden sollen.	`[{"sortPriority":"1", "sortAscending":"true", "id":"kpi.NAME"}]`
Angepasste KPI-Farben	Im Portlet verwendete Farben, um den Status von KPIs anzuzeigen. Beispieleingabe: `{"acceptable":"#7f7f7f", "take_action":"#34333"}` Die hier eingegebenen Farben setzen die von der Lösung bereitgestellten Farben außer Kraft.	{}
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`KpiDrillDownPortletHelp`

Tabelle 46. Anpassungsparameter des Key Performance Indicator - Drilldown-Portlets (Forts.)

Enable KPI filter	Einstellung des Typs "true" (Wahr) oder "false" (Falsch), um einen KPI-Filter entsprechend den Informationen in der Parametereinstellung **KPI filter** (KPI-Filter) zu aktivieren oder zu inaktivieren.	`false`
Hide toolbar (Symbolleiste ausblenden)	Einstellung des Typs "Wahr" oder "Falsch", um die Symbolleiste oben im Portlet aus- oder einzublenden.	`true`
KPI filter (KPI-Filter)	Kennungen von KPIs, die angezeigt werden, wenn der Parameter **Enable KPI filter** (KPI-Filter aktivieren) für das Portlet auf `true` gesetzt ist. Beispieleingabe: `["Transportation","Airports", "Roads_and_Traffic", "Public_Safety","Fire_Department", "Water","Delayed_Flights", "Delayed_Flights_Airport_Two"]`	`[]`
Portlet group identifier (Portletgruppen-ID)	Name der Gruppe, der dieses Portlet angehört. Ein allgemeiner Name richtet die Datenübertragung zwischen den Portlets "Key Performance Indicator - Drilldown" und "Status" auf derselben Seite ein.	`default`
Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	`350`
Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	`600`
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der folgende von der Lösung bereitgestellte Titel angezeigt: Key Performance Indicator - Drilldown.
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.

Anmerkung: Die Erläuterung des Ereignisses für den Portlet-Titel beim Bereitstellen eines Ressourcenpakets gilt gleichermaßen für den Spaltentitel, der aus demselben Ressourcenpaket stammt.

Spaltenparameter (columns)

Der Wert des Parameters **columns** (Spalten) ist eine Gruppe von JSON-Objekten, die entsprechend den Erklärungen in der folgenden Tabelle konfiguriert werden können.

Tabelle 47. Objekte innerhalb des Wertes des Spaltenparameters des Key Performance Indicator - Drilldown-Portlets

Objekt	Enthält
`sortPriority`	• Zahl, um die Sortierpriorität dieser Spalte im Vergleich zu allen anderen Spalten anzugeben, wobei die Priorität umso höher ist, je kleiner die Zahl ist • Kein Wert, leer lassen, um die Standardeinstellung der Sortierpriorität der Spalte zu verwenden • `-1`, um die Standardeinstellung der Sortierpriorität der Spalte zu inaktivieren
`sortAscending`	• `true`, um eine aufsteigende Sortierreihenfolge für die Spalteneinträge zu verwenden • `false`, um eine absteigende Sortierreihenfolge für die Spalteneinträge zu verwenden
`id`	die Spalten-ID, um anzuzeigen, dass die Spalte angezeigt werden soll

Spalten werden im Portlet in derselben Reihenfolge angezeigt wie in den JSON-Objekten angegeben, die den Wert des Parameters **`columns`** bilden. Es werden nur die Spalten angezeigt, deren Spalten-ID innerhalb des Wertes liegt. Alle anderen Spalten sind ausgeblendet. Wenn für den Parameter **`columns`** kein Wert angegeben wird, werden die Spalten entsprechend der Standardeinstellung angezeigt, die in der ersten Zeile von Tabelle 46 auf Seite 161 dargestellt ist.

Die gültigen Werte für die Spalten-IDs sind in der folgenden Tabelle beschrieben.

Tabelle 48. Gültige Spalten-IDs des Key Performance Indicator - Drilldown-Portlets

Spalten-ID	Beschreibung
`kpi.NAME`	Name des KPI
`kpi.CURRENT.VALUE`	Aktueller Wert des KPI
`kpi.CURRENT.STATUS`	Aktueller Status des KPI
`kpi.CALCULATION.TIME`	Zeit, zu der der KPI berechnet wurde

Zugehörige Konzepte:

„Key Performance Indicator - Drilldown" auf Seite 290
Mit dem Portlet "Key Performance Indicator - Drilldown" können Sie weitere Informationen zu einer KPI-Kategorie, den Status der untergeordneten KPIs anzeigen.

Einstellungen des Key Performance Indicators (KPIs)-Portlets

Anpassen des Key Performance Indicators (KPIs)-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Key Performance Indicators (KPIs)-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 49. Anpassungsparameter des Key Performance Indicators (KPIs)-Portlets

Parameter	Beschreibung	Standardwert
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`KpiManagerPortletHelp`

Tabelle 49. Anpassungsparameter des Key Performance Indicators (KPIs)-Portlets (Forts.)

Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	`500`
Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	`600`
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der folgende von der Lösung bereitgestellte Titel angezeigt: Key Performance Indicators (KPIs).
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.

Zugehörige Konzepte:

„Key Performance Indicators (KPIs)" auf Seite 178
Mit dem Portlet "Key Performance Indicators (KPIs)" können Sie KPIs (Key Performance Indicator) und ihre hierarchische Anzeige in IBM Intelligent Operations Center anpassen.

Einstellungen des Positionskarte-Portlets

Anpassen des Positionskarte-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 50. Werte der Anpassungsparameter des Positionskarte-Portlets

Parameter	Beschreibung	Standardwert
Default filter selections (Standardfilterauswahl)	Standardmäßige Ereigniskategorien, die auf der Karte angezeigt werden sollen. Geben Sie den Namen oder mehrere Namen ein, die durch ein Semikolon ohne Leerzeichen getrennt werden müssen.	`CBRNE;Env;Fire;Geo;Health; Infra;Met;Rescue;Safety;Security; Transport;Other`
Standardmäßige Farbe zur Hervorhebung von Bereichen	Standardmäßige Farbe eines Bereichs, der hervorgehoben wird, wenn Sie den Cursor über dem Bereich bewegen.	`#808080`
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`LocationMapPortletHelp`
Standardmäßige Kartenauswahl	Name der Standardpositionskarte, die im Portlet angezeigt werden soll.	`Miami SunLife Stadium`
Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	`600`

Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	400
Portlet group identifier (Portletgruppen-ID)	Name der Gruppe, der dieses Portlet angehört. Ein allgemeiner Name richtet die Datenübertragung zwischen den Portlets "Karte", "Details" und "Positionskarte" auf derselben Seite ein.	default
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der folgende von der Lösung bereitgestellte Titel angezeigt: Positionskarte.
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.

Zugehörige Konzepte:

„Positionskarte” auf Seite 291
Mit dem Portlet "Positionskarte" können Sie die auf einer Positionskarte markierten Ereignisse anzeigen. Eine Positionskarte im IBM Intelligent Operations Center ist eine Karte oder ein Plan mit vordefinierten Interaktionsbereichen, wie z. B. Sitzbereiche in großen Sportstadien.

Einstellungen des Positionskartenmanager-Portlets

Anpassen des Positionskartenmanager-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 51. Werte der Anpassungsparameter des Positionskartenmanager-Portlets

Parameter	Beschreibung	Standardwert
Default color for selected new area (Standardfarbe für den ausgewählten neuen Bereich)	Standardfarbe eines Bereichs, der auf der Karte gezeichnet und ausgewählt wurde.	#4AA02C
Default color for selected saved area (Standardfarbe für einen ausgewählten gespeicherten Bereich)	Standardfarbe eines Bereichs auf der Karte, der gespeichert und ausgewählt wurde.	#808080
Default color for new area (Standardfarbe für einen neuen Bereich)	Standardfarbe eines Bereichs, der auf der Karte gezeichnet wurde.	#009900
Default color for saved area (Standardfarbe für einen gespeicherten Bereich)	Standardfarbe eines Bereichs, der auf der Karte gespeichert wurde.	#808080

Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`LocationMapManagerPortletHelp`
Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	`400`
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der folgende von der Lösung bereitgestellte Titel angezeigt: Positionskartenmanager.
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.

Zugehörige Konzepte:

„Positionskartenmanager" auf Seite 186
Mithilfe des Portlets "Positionskartenmanager" können Sie das Portlet "Positionskarte" anpassen.

Einstellungen des Karte-Portlets

Anpassen des Karte-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Karte-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 52. Werte der Anpassungsparameter

Parameter	Beschreibung	Standardwert
Breitengrad des Mittelpunkts	Bestimmte Koordinaten, um den Mittelpunkt der Karte festzulegen. Die aktuelle Position der Karte wird rechts von den Feldern angezeigt. Sie können die Karte zu Ihrer gewünschten Position zoomen oder schwenken und anschließend die in den entsprechenden Feldern gezeigten Werte ausschneiden und einfügen.	`25,780416`
Längengrad des Mittelpunkts		`-80,203629`

Tabelle 52. Werte der Anpassungsparameter (Forts.)

Zoomstufe	Standardmäßige Vergrößerungsstufe für die Karte. Die Anzahl verfügbarer gültiger Zoomstufen hängt von der Basiskarte ab. Üblicherweise liegt die Anzahl bei 1 oder höher. Der Wert 1 entspricht der niedrigsten Zoomstufe, mit der die Karte in der geringsten Vergrößerung angezeigt wird. Die mit der Lösung bereitgestellte, standardmäßige ArcGIS-Basiskarte zeigt z. B. geografische Details bis zu einer maximalen Zoomstufe von 12 an.	11
Typ der Basisebene	Wert für den Typ der Basiskarte.	`ARC_GIS_REST`
URL der Basisebene	URL der Basiskarte. Die URL muss - in der korrekten Reihenfolge - die Platzhalter enthalten, die die Koordinaten x, y und z der Karte darstellen. Sie können eine Karte von Ihrem installierten Esri GIS-Server oder einen frei verfügbaren GIS-Service verwenden.	`http://services.arcgisonline.com/ArcGIS/rest/services/World_Street_Map/MapServer/tile/${z}/${y}/${x}`
KML-Feed oder Datei-URL	URL, um KML-Daten anzuzeigen. Geben Sie eine URL mit derselben Domäne und demselben Port für eine Position auf demselben Server ein wie das Portlet. Um sicherzustellen, dass Sie diese Bedingung implementieren, geben Sie nur URLs ein, die mit einem Schrägstrich ('/') beginnen, damit der Browser die aktuelle Domäne und den aktuellen Port auswählt. Verwenden Sie für mehrere URL-Zeichenfolgen ein Semikolon und keine Leerzeichen zwischen URLs. Wenn die erforderliche Website nicht lokal ist, verwenden Sie einen Proxy-Server auf Ihrem Portalserver, um auf die Site zuzugreifen. **Anmerkung:** Verwenden Sie diese Option für geringfügige lokale Anpassungen, aber beachten Sie die einbezogenen Datenmengen, damit diese nicht die Anzeige überfrachten oder die Leistung beeinträchtigen.	Von der Lösung wird kein Standardwert bereitgestellt.

Tabelle 52. Werte der Anpassungsparameter (Forts.)

Die Anzahl der angezeigten Elemente	Grenze für die Anzahl der in einer Ansicht angezeigten Markierungen. Geben Sie die maximale Anzahl von Markierungen ein, die angezeigt werden können. Wenn die Anzahl der Markierungen in dem angezeigten Bereich der Karte diese Grenze übersteigt, werden keine Markierungen abgebildet und es wird ein Warnhinweis angezeigt. Der Benutzer kann dann wählen, ob er die Markierungen laden oder die Ansicht ändern möchte.	`250`

Default filter selections (Standardfilterauswahl)	Standardmäßige Ereigniskategorien, die auf der Karte angezeigt werden sollen. Geben Sie den Namen oder mehrere Namen ein, die durch ein Semikolon ohne Leerzeichen getrennt werden müssen.	`CBRNE;Env;Fire;Geo;`
		`Health;Infra;Met;Rescue;`
		`Safety;Security;Transport;`
		`Other`

Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	`600`
Portlet group identifier (Portletgruppen-ID)	Name der Gruppe, der dieses Portlet angehört. Ein allgemeiner Name richtet die Datenübertragung zwischen den Portlets "Karte", "Details" und "Positionskarte" auf derselben Seite ein.	`default`
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der folgende von der Lösung bereitgestellte Titel angezeigt: Karte.
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`NavigatorPortletHelp`
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.

Zugehörige Konzepte:

„Karte” auf Seite 294
Mit dem Portlet "Karte" können Sie die in einer Karte enthaltenen Ereignisse und Ressourcen anzeigen.

Einstellungen des Meine Aktivitäten-Portlets

Anpassen des Meine Aktivitäten-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Meine Aktivitäten-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 53. Anpassungsparameter des Meine Aktivitäten-Portlets

Parameter	Beschreibung	Standardwert
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`ActivitiesPortletHelp`
Portlet group identifier (Portletgruppen-ID)	Name der Gruppe, der dieses Portlet angehört. Ein allgemeiner Name richtet die Datenübertragung zwischen Portlets auf derselben Seite ein. Ein allgemeiner Name kann beispielsweise die Datenübertragung zwischen den Portlets "Meine Aktivitäten" und "Details" einrichten.	`default`
Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	`200`
Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	`600`
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der folgende von der Lösung bereitgestellte Titel angezeigt: Meine Aktivitäten.
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.

Zugehörige Konzepte:

„Meine Aktivitäten” auf Seite 300
Im Portlet "Meine Aktivitäten" wird eine dynamische Liste mit Aktivitäten angezeigt, deren Eigner die Gruppe ist, zu der der an der Schnittstelle angemeldete Benutzer gehört.

Einstellungen des Benachrichtigungen-Portlets

Anpassen des Benachrichtigungen-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Benachrichtigungen-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 54. Anpassungsparameter des Benachrichtigungen-Portlets

Parameter	Beschreibung	Standardwert
Columns (Spalten)	Spezifikationen und die Reihenfolge der Spalten, die in der Liste angezeigt werden sollen.	`[{"id": "notifications.HEADLINE"},{"id": "notifications.SENTFROM"},{"id": "notifications.SENTTIME", "width" : "10", "format": "yyyy-MM-dd HH:mm:ss"}]`
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`CityCoordinatorPortletHelp`
Hide toolbar (Symbolleiste ausblenden)	Einstellung des Typs "Wahr" oder "Falsch", um die Symbolleiste oben im Portlet aus- oder einzublenden.	`true`
Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	`200`
Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	`600`
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der folgende von der Lösung bereitgestellte Titel angezeigt: Benachrichtigungen.
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.

Anmerkung: Die Erläuterung des Ereignisses für den Portlet-Titel beim Bereitstellen eines Ressourcenpakets gilt gleichermaßen für den Spaltentitel, der aus demselben Ressourcenpaket stammt.

Spaltenparameter

Der Wert des Parameters **`columns`** (Spalten) ist eine Gruppe von JSON-Objekten, die entsprechend den Erklärungen in Tabelle 55 konfiguriert werden können.

Tabelle 55. Objekte innerhalb des Wertes des Spaltenparameters des Benachrichtigungen-Portlets

Objekt	Enthält
`id`	die Spalten-ID, um anzuzeigen, dass die Spalte angezeigt werden soll
`width`	Anzahl der Pixel, die die Spaltenbreite angibt.

Tabelle 55. Objekte innerhalb des Wertes des Spaltenparameters des Benachrichtigungen-Portlets (Forts.)

Objekt	Enthält
`format`	Zeichenfolge, die das Format darstellt, das für die Datums- und Uhrzeitspalten zu verwenden ist, wobei der Eintrag die Einstellung in der Tabelle `sysprop` außer Kraft setzt
`sortAscending`	• `true`, um eine aufsteigende Sortierreihenfolge für die Spalteneinträge zu verwenden • `false`, um eine absteigende Sortierreihenfolge für die Spalteneinträge zu verwenden
`sortPriority`	• Zahl, um die Sortierpriorität dieser Spalte im Vergleich zu allen anderen Spalten anzugeben, wobei die Priorität umso höher ist, je kleiner die Zahl ist • Kein Wert, leer lassen, um die Standardeinstellung der Sortierpriorität der Spalten zu verwenden • `-1`, um die Standardeinstellung der Sortierpriorität der Spalten zu inaktivieren
`title`	Spaltenüberschrift, die nicht zu belegen ist, wenn die Standardüberschrift verwendet werden soll

Spalten werden im Portlet in derselben Reihenfolge angezeigt wie in den JSON-Objekten, die den Wert des Parameters **`columns`** bilden, angegeben. Es werden nur die Spalten angezeigt, deren Spalten-ID innerhalb des Wertes liegt. Alle anderen Spalten sind ausgeblendet. Wenn der Wert des Parameters **`columns`** übergangen wird, werden die Spalten entsprechend der Standardeinstellung angezeigt, die in der ersten Zeile von Tabelle 54 auf Seite 170 dargestellt ist.

Die gültigen Werte für die Spalten-IDs sind in Tabelle 56 beschrieben.

Tabelle 56. Gültige Spalten-IDs des Benachrichtigungen-Portlets

Spalten-ID	Beschreibung
`notifications.ID`	die UUID der Benachrichtigung in der Benachrichtigungstabelle
`notifications.CATEGORY`	Nicht übersetzter Wert der mit der Benachrichtigung verbundenen Kategorie des Ereignisses oder des KPI
`notifications.SENTFROM`	Service, der die Benachrichtigung generiert hat
`notifications.SENTTOGROUP`	Liste der Gruppen, die auf die Benachrichtigung zugreifen können
`notifications.SENTTIME`	Zeit, die von dem Service, der die Benachrichtigung gesendet hat, erfasst wurde
`notifications.HEADLINE`	Kurzer Text zur Beschreibung der Benachrichtigung
`notifications.DESCRIPTION`	Ausführlicher Text zur Beschreibung der Benachrichtigung
`notifications.ALERTLINK`	Liste von CAP-Alerts, die in Beziehung zur Benachrichtigung stehen
`notifications.KPILINK`	KPI, das in Beziehung zur Benachrichtigung steht

Zugehörige Konzepte:

„Benachrichtigungen" auf Seite 302
Mit dem Portlet "Benachrichtigungen" können Sie Alertnachrichten sowie Details zu diesen Nachrichten anzeigen.

Einstellungen des Berichte-Portlets

Anpassen des Berichte-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 57. Werte der Anpassungsparameter des Berichte-Portlets

Parameter	Beschreibung	Standardwert
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`ReportsIntegrationPortletHelp`
Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	`600`
Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	`800`
Portlet title (Portlet-Titel)	Titel des Berichte-Portlet.	`Benutzerdefinierter Bericht`
Report URL (Berichts-URL)	Gibt die URL des angezeigten Berichts an.	`http://ioc1bvtlite1.rtp.raleigh.ibm.com/cognos/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run&ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_cap_model%27%5d%2ffolder%5b%40name%3d%27reports%27%5d%2ffolder%5b%40name%3d%27User_defined_reports%27%5d%2freport%5b%40name%3d%27User_defined_report%27%5d&ui.name=User_defined_report&run.outputFormat=&run.prompt=true&cv.toolbar=false&cv.header=false`
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das Sie als Quelle für den Eigenschaftenwert bereitstellen, z. B. der Portlet-Titel. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben wird, wird nicht nach dem Schlüssel gesucht und der Titel wird angezeigt, wie im Feld Portlet title (Portlet-Titel) des Fensters **Gemeinsam genutzte Einstellungen** dargestellt.	Es gibt kein standardmäßiges Ressourcenpaket.

Tabelle 57. Werte der Anpassungsparameter des Berichte-Portlets (Forts.)

Show URL field on page (URL-Feld auf Seite anzeigen)	Wählen Sie **True** (Wahr) aus, um die Schaltfläche **Report URL** (Berichts-URL) in die Portletseite "Berichte" einzuschließen. Mithilfe der Schaltfläche können alle Benutzer, nicht nur Administratoren, einen benutzerdefinierten Bericht erstellen und die Berichts-URL festlegen. Wählen Sie **False** (Falsch) aus, um die Schaltfläche **Report URL** (Berichts-URL) aus der Portletseite "Berichte" auszuschließen.	`False`

Zugehörige Konzepte:

„Berichte" auf Seite 304

Mit dem Portlet "Berichte" können Berichte von Ereignissen in Form von Diagrammen angezeigt werden. In diesem Portlet gibt es mehrere Möglichkeiten für die Anordnung von Ereignissen; darüber hinaus können Ereignisse nach einem bestimmten Datum oder Zeitraum ausgewählt werden. Mithilfe dieser Berichte können Sie Maßnahmen für aktuelle und künftige Ereignisse planen.

Einstellungen des Beispiel-Publisher-Portlets

Anpassen des Beispiel-Publisher-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Beispiel-Publisher-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 58. Anpassungsparameter des Beispiel-Publisher-Portlets

Parameter	Beschreibung	Standardwert
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`SamplePublisherPortletHelp`
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der folgende von der Lösung bereitgestellte Titel angezeigt: Beispiel-Publisher.
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.

Zugehörige Konzepte:

„Beispiel-Publisher" auf Seite 110
Mit dem Portlet "Beispiel-Publisher" können CAP-Ereignisse (Common Alerting Protocol) in IBM Intelligent Operations Center veröffentlicht werden.

Einstellungen des Standard Operating Procedures-Portlets

Anpassen des Standard Operating Procedures-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Standard Operating Procedures-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 59. Anpassungsparameter des Standard Operating Procedures-Portlet

Parameter	Beschreibung	Standardwert
Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`SOPManagerPortletHelp`
Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	`440`

Zugehörige Konzepte:

„Standard Operating Procedures" auf Seite 135
Für die Verwaltung von Ereignissen, die im IBM Intelligent Operations Center auftreten, können Sie Standard Operating Procedures und Aktivitäten definieren. Verwenden Sie das Portlet "Standard Operating Procedures", um auf Standard Operating Procedure, Auswahlmatrix für Standard Operating Procedure und Workflow-Designer-Anwendungen in Tivoli Service Request Manager zuzugreifen.

Einstellungen des Status-Portlets

Anpassen des Status-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Anpassungsparameter

Die Felder des Fensters **Gemeinsam genutzte Einstellungen** enthalten die Werte der Anpassungsparameter für das Status-Portlet. Die Anpassungsparameter sind in der folgenden Tabelle beschrieben.

Tabelle 60. Anpassungsparameter des Status-Portlets

Parameter	Beschreibung	Standardwert

Angepasste KPI-Farben	Im Portlet zu verwendende Farben, um den Status von KPIs anzuzeigen. Beispieleingabe:
	`{"acceptable":"#7f7f7f",`
	`"take_action":"#34333"}`
	
	Die hier eingegebenen Farben setzen die von der Lösung bereitgestellten Farben außer Kraft.
		{}

Default help JSP (Standardmäßige JSP-Hilfe)	Name der JSP-Hilfedatei, der angezeigt werden soll, wenn die Hilfe im Portletmenü ausgewählt wird.	`KpiStatusPortletHelp`
KPI-Filter aktivieren	Einstellung des Typs "true" (Wahr) oder "false" (Falsch), um einen KPI-Filter entsprechend den Informationen im Wert des Parameters **`KPI filter`** KPI-Filter zu aktivieren oder zu inaktivieren.	`false`

Tabelle 60. Anpassungsparameter des Status-Portlets (Forts.)

KPI-Filter	Kennungen von KPIs, die angezeigt werden, wenn der Parameter "Enable KPI filter" (KPI-Filter aktivieren) für das Portlet auf "true" gesetzt ist, z. B.: `["Transportation","Airports", "Roads_and_Traffic","Public_Safety", "Fire_Department", "Water","Delayed_Flights", "Delayed_Flights_Airport_Two"]`	`[]`
Portlet group identifier (Portletgruppen-ID)	Name der Gruppe, der dieses Portlet angehört. Ein allgemeiner Name richtet die Datenübertragung zwischen den Portlets "Key Performance Indicator - Drilldown" und "Status" auf derselben Seite ein.	`default`
Portlet height (Portlethöhe)	Anzahl der Pixel, die die Standardhöhe des Portlets angeben.	`200`
Portlet maximum height (Maximale Portlethöhe)	Anzahl der Pixel, die die maximale Höhe für das Portlet angeben.	`600`
Portlet title (Portlet-Titel)	Titel, mit dem der mit der Lösung bereitgestellte Titel überschrieben wird.	Wenn Sie keinen Wert für diesen Parameter eingeben, wird der folgende von der Lösung bereitgestellte Titel angezeigt: Status.
Resource bundle (Ressourcenpaket)	Position des Ressourcenpakets, das als Quelle für den Wert von Eigenschaften wie dem Portlettitel bereitgestellt wird. Diese Position ist erforderlich, wenn Sie den Titel als Eigenschaftsschlüssel in einem bereitgestellten Ressourcenpaket angeben möchten. Wenn kein Ressourcenpaket angegeben ist, wird nicht nach dem Schlüssel gesucht, und der von der Lösung bereitgestellte Titel wird angezeigt.	Es gibt kein standardmäßiges Ressourcenpaket.
Show legend (Legende anzeigen)	Einstellung des Typs "Wahr" oder "Falsch", um die Legende im Portlet aus- oder einzublenden.	`true`
Sortierreihenfolge	KPI-Eigenschaft, nach der die KPI-Liste sortiert ist. In der Standardeinstellung wird in aufsteigender alphabetischer Reihenfolge nach KPI-Name sortiert. Andere Optionen sind `kpi.CURRENT.VALUE`, `kpi.CURRENT.STATUS` und `kpi.CALCULATION.TIME`	`+kpi.NAME`

Zugehörige Konzepte:

„Status" auf Seite 306
Mit dem Portlet "Status" können Sie den Status von KPIs einer einzelnen Einrichtung oder mehrerer Einrichtungen anzeigen.

Portlethilfe anpassen

Sie können eine alternative Hilfe für ein IBM Intelligent Operations Center-Portlet implementieren.

Informationen zu diesem Vorgang

Klicken Sie im Portlet in die rechte obere Ecke und wählen Sie aus dem angezeigten Menü **Hilfe** aus, um das Hilfemenü in dem jeweiligen Portlet aufzurufen.

Wenn Sie das Layout oder die in einem Portlet angezeigten Daten ändern, möchten Sie möglicherweise auch die angezeigte Hilfe ändern.

Vorgehensweise

1. Erstellen Sie die alternative Hilfe als JSP-Datei.
2. Sie können der Datei einen beliebigen Namen zuordnen, jedoch müssen Sie das korrekte Suffix für Ihre Sprache verwenden. Die Spracheinstellung basiert auf der Sprache Ihres Browsers. Verwenden Sie die Standard-ID der Ländereinstellung für Ihre Sprache, z. B.:

Option	Bezeichnung
_pt_BR	Portugiesisch (Brasilien)
_en	Englisch
_fr	Französisch
_de	Deutsch
_es	Spanisch

3. Verwenden Sie das Portlet **Shared Settings** (Gemeinsame Einstellungen), um den Parameter **`DefaultHelpJSP`** mit dem Namen der alternativen Hilfedatei festzulegen. Fügen Sie nicht das Sprachsuffix oder die Dateierweiterung ".jsp" hinzu.
4. Kopieren Sie die alternative JSP-Hilfedatei in das korrekte Verzeichnis: `/opt/IBM/WebSphere/wp_profile/installedApps/cell1/ioc_portal_ear.ear/`*`Portlet-WAR`*`/`*`Portlet-Root`*`/jsp/html/help`. Die jeweiligen Portletwerte für die Variablen *Portlet-WAR* und *Portlet-Root* sind in einem separaten Thema aufgelistet. Eine Liste dieser Werte erhalten Sie über den Link am Ende dieses Themas.

   Anmerkung: Wenn Sie die Hilfedatei für Zusammenfassung der Benutzerberechtigungen ändern, ersetzen Sie `ioc_portal_ear.ear` durch `iss_portal_ear.ear` in dem in diesem Schritt angegebenen Pfad.

Nächste Schritte

Stellen Sie Übersetzungen der alternativen Hilfedatei für alle unterstützten Sprachen einschließlich einer Standardsprache bereit.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Positionen der Portlet-Hilfedateien

Positionswerte sind für jedes Portlet erforderlich, wenn Sie die Portlet-Standardhilfe durch eine alternative JSP-Hilfedatei ersetzen.

In Tabelle 1 und 2 sind Werte für Hilfedateien der Benutzer- und Verwaltungsportlets enthalten.

Tabelle 61. Benutzerportletwerte für die Position einer alternativen Hilfedatei

Portlet	*Portlet-WAR*	*Portlet-Root*
Details	icoc_ui_common_events_portlet.war	_icoc_ui_common_events_portlet
Key Performance Indicator - Drilldown	icoc_ui_kpi_drilldown_portlet.war	_icoc_ui_kpi_drilldown_portlet
Positionskarte	icoc_ui_location_map_portlet.war	_icoc_ui_location_map_portlet
Karte	icoc_ui_navigator_portlet.war	_icoc_ui_navigator_portlet
Meine Aktivitäten	icoc_ui_activities_portlet.war	_icoc_ui_activities_portlet
Benachrichtigungen	icoc_ui_city_coordinator_portlet.war	_icoc_ui_city_coordinator_portlet
Berichte	icoc_ui_reports_portlet.war	_icoc_ui_reports_portlet
Status	icoc_ui_kpi_status_portlet.war	_icoc_ui_kpi_status_portlet

Tabelle 62. Verwaltungsportletwerte für die Position einer alternativen Hilfedatei

Portlet	*Portlet-WAR*	*Portlet-Root*
Administrations-konsolen	icoc_ui_administration_console_portlet.war	_icoc_ui_administration_console_portlet
Erstellung von Ereignisscripts	icoc_ui_event_scripting_portlet.war	_icoc_ui_event_scripting_portlet
Key Performance Indicators (KPIs)	icoc_ui_kpi_manager_portlet.war	_icoc_ui_kpi_manager_portlet
Positionskarten-manager	icoc_ui_location_map_manager_portlet.war	_icoc_ui_location_map_manager_portlet
Beispiel-Publisher	icoc_ui_sample_publisher_portlet.war	_icoc_ui_sample_publisher_portlet
Standard Operating Procedures	icoc_ui_sop_manager_portlet.war	_icoc_ui_sop_manager_portlet
Zusammenfassung der Benutzer-berechtigungen	iss_ui_security_portlet.war	_iss_ui_security_portlet

KPIs anpassen

Im IBM Intelligent Operations Center können Sie KPI-Modelle (Key Performance Indicator-Modelle) an Ihre Geschäftsprozesse anpassen.

KPIs wurden dafür entwickelt, statistische Daten bereitzustellen, die zur Analyse von Trends oder zur Anzeige von Problembereichen verwendet werden können. KPI-Daten werden durch Ereignisse innerhalb des IBM Intelligent Operations Center aktualisiert.

Das IBM Intelligent Operations Center stellt eine Reihe von Beispiel-KPIs und -Ereignissen bereit, die verwendet werden können, um den KPI-Status zu aktualisieren. Mit dem IBM Intelligent Operations Center werden drei KPI-Beispielmodelle bereitgestellt, die auf Beispielen aus den Bereichen öffentliche Sicherheit, Transportwesen und Wasserversorgung und Geschäftsprozessen beruhen. Weitere Informationen zu mit dem IBM Intelligent Operations Center bereitgestellten Beispiel-KPIs finden Sie unter dem Link am Ende dieses Themas.

Jede IBM Intelligent Operations Center-Lösung folgt einem KPI-Erstellungs- und Integrationsprozess, der dazu dient, die KPIs einzustellen, die für das jeweilige Geschäftsumfeld erforderlich sind. Sie können mit dem IBM WebSphere Business Monitor Ihre eigenen KPI-Modelle erstellen. Weitere Informationen zur Erstellung und Integration von KPIs mithilfe des IBM Intelligent Operations Center finden Sie unter dem Link am Ende dieses Themas.

Verwenden Sie das Key Performance Indicators (KPIs)-Portlet, um KPIs im IBM Intelligent Operations Center anzupassen. Das Key Performance Indicators (KPIs)-Portlet wird dem Administrator als eine der Optionen der **Tools zur Anpassung der Lösung** bereitgestellt.

Unter Verwendung des Portlets können Sie Eigenschaften von KPIs anzeigen, KPIs erstellen, kopieren oder ändern und Anzeigehierarchien für KPI-Modelle anzeigen oder ändern.

Verwenden Sie die Registerkarte **KPI-Definition**, um die KPIs zu definieren, die einem bestimmten KPI-Modell im IBM Intelligent Operations Center zugeordnet sind:

- Die aktuelle Liste der KPIs anzeigen, die zu einem KPI-Modell gehören.
- Die Eigenschaften eines vorhandenen KPIs anzeigen.
- Die Eigenschaften eines vorhandenen KPIs aktualisieren.
- Einen neuen KPI für ein KPI-Modell erstellen:
  - Mithilfe einer definierten Metrik berechneter Aggregat-KPI
  - Auf anderen KPIs basierender Wert eines Ausdrucks-KPIs

- Einen KPI löschen.

Ihre Updates werden in IBM WebSphere Business Monitor-Modellen gespeichert, die in der Datenbank des IBM Intelligent Operations Center abgelegt sind. Ihre Updates werden auch bei der nächsten Aktualisierung der Status- und Key Performance Indicator - Drilldown-Portlets wiedergegeben.

Verwenden Sie die Registerkarte **KPI-Anzeigehierarchie anzeigen**, um die KPI-Hierarchien zu aktualisieren, die in den Status- und Key Performance Indicator - Drilldown-Portlets angezeigt werden.

- Die vorhandenen KPI-Hierarchien anzeigen.
- Die Haupteigenschaften eines KPI anzeigen.
- Die Baumstruktur durch Verschieben oder Entfernen von Elementen in einer KPI-Hierarchie verändern.
- Vordefinierte KPIs zu einer Hierarchie hinzufügen.

Ihre Updates werden bei der nächsten Aktualisierung der Status- und Key Performance Indicator - Drilldown-Portlets wiedergegeben.

Anmerkung: Alle Updates der Anzeigehierarchie sind unabhängig vom KPI-Modell. Ein Verständnis des KPI-Modells ist erforderlich, um sicherzustellen, dass Updates mit der Logik des KPI-Modells übereinstimmen.

Zugehörige Konzepte:

„KPIs erstellen und integrieren" auf Seite 116
KPI-Modelle (Key Performance Indicator) können mit einem Entwicklungstoolkit zur Geschäftsüberwachung und einem KPI-Managementportlet erstellt und geändert werden.

„Beispiel-KPIs" auf Seite 129
Im Rahmen des IBM Intelligent Operations Center werden auch Beispiel-KPIs zur Verfügung gestellt. Die Beispiel-KPIs dienen als Anhaltspunkt und sollen Sie bei der Implementierung verschiedener KPI-Typen mit dem IBM WebSphere Business Monitor Development Toolkit unterstützen. Es werden Beispielüberwachungsmodelle aus dem Bereich Wasser, Transport und öffentliche Sicherheit bereitgestellt.

Key Performance Indicators (KPIs)

Mit dem Portlet "Key Performance Indicators (KPIs)" können Sie KPIs (Key Performance Indicator) und ihre hierarchische Anzeige in IBM Intelligent Operations Center anpassen.

Im Portlet "Key Performance Indicators (KPIs)" können Sie KPIs anzeigen, ändern, kopieren, erstellen und löschen. Darüber hinaus können Sie die in den Portlets "Status" und "Key Performance Indicator - Drilldown" angezeigten KPI-Hierarchien anpassen.

Um auf das Portlet "Key Performance Indicators (KPIs)" zuzugreifen, klicken Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Customization Tools** > **Key Performance Indicators** (Intelligent Operations > Anpassungstools > Key Performance Indicators).

KPI-Hierarchien anzeigen

Auf der Registerkarte **Beziehungen und Anzeige** können Sie die KPI-Modelle anzeigen, die in den Portlets "Status" und "Key Performance Indicator - Drilldown" angezeigt werden.

Informationen zu diesem Vorgang

Links im Fenster **Beziehungen und Anzeige** sind die Knoten auf Stammebene der KPI-Hierarchien zu sehen, zu deren Anzeige Sie berechtigt sind. Diese Knoten stellen die KPI-Modelle dar, wie sie in den Portlets "Status" und "Key Performance Indicator - Drilldown" angezeigt werden.

Vorgehensweise

1. Erweitern Sie einen Knoten auf Stammebene, um die unteren Ebenen der Modellbaumstruktur einzublenden, die angezeigt werden sollen.

2. Klicken Sie auf den Titel eines Knotens auf Stammebene, um im rechten Fenster Details zu dem betreffenden Knoten anzuzeigen. Die Informationen werden wie in der folgenden Tabelle beschrieben angezeigt:

Option	Bezeichnung
Name	Titel des Knotens auf Stammebene
Typ	Typ des Knotens auf Stammebene
Modell-ID	ID für das entsprechende KPI-Modell
Kategorie	Klassifikation des Modells
Symbol	Symbol für den Knoten auf Stammebene

3. Klicken Sie auf einen KPI, um rechts im Fenster **Beziehungen und Anzeige** Details zu dem jeweiligen KPI anzuzeigen.

KPI-Hierarchien ändern

Auf der Registerkarte **Beziehungen und Anzeige** können Sie ein in den Portlets "Status" und "Key Performance Indicator - Drilldown" angezeigtes KPI-Modell ändern oder entfernen.

Vorgehensweise

1. Klicken Sie links im Fenster **Beziehungen und Anzeige** auf den Knoten auf Stammebene und auf die jeweils untergeordneten Elemente, bis sie zu der gewünschten Ebene in der hierarchischen Baumstruktur gelangen.
2. So können Sie Elemente verschieben, hinzufügen, ändern oder entfernen:
   - Sollen untergeordnete Elemente innerhalb einer Baumstruktur verschoben werden, ziehen Sie das Element an die gewünschte Position. Grüne oder rote Indikatoren zeigen an, ob eine Verschiebung zulässig ist oder nicht.
   - Soll einer Baumstruktur ein Element aus der Liste vorhandener untergeordneter Elemente für ein KPI-Modell hinzugefügt werden, klicken Sie mit der rechten Maustaste auf das Element, in das das untergeordnete Element eingefügt werden soll, und klicken Sie auf **KPI hinzufügen**.
   - Soll das Fenster mit den KPI-Eigenschaften geöffnet werden, um ein untergeordnetes Element zu ändern, klicken Sie mit der rechten Maustaste auf das Element und klicken Sie auf **Bearbeiten**.
   - Soll ein Knoten auf Stammebene oder ein untergeordnetes Element aus einer Baumstruktur entfernt werden, klicken Sie mit der rechten Maustaste auf das Element und klicken Sie anschließend auf **Entfernen**. Bei Entfernen eines Stammknotens werden alle in diesem Knoten enthaltenen untergeordneten Elemente entfernt.
3. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

   Anmerkung: Der Name einer Eignereinrichtung oder eines Knotens auf Stammebenen kann hier nicht geändert werden. Soll eine Eignereinrichtung geändert werden, müssen Sie sie entfernen und durch einen anderen Namen ersetzen.

Eignereinrichtung hinzufügen

Auf der Registerkarte **Beziehungen und Anzeige** können Sie einen Knoten auf Stammebene hinzufügen, der in den Portlets "Status" und "Key Performance Indicator - Drilldown" angezeigt werden soll.

Vorgehensweise

1. Klicken Sie links oben im Fenster **Beziehungen und Anzeige** auf **Eignereinrichtung hinzufügen**.
2. Geben Sie einen Anzeigenamen ein.
3. Wählen Sie in der Dropdown-Liste des Feldes **Modell** den Knoten auf Stammebene aus, der hinzugefügt werden soll.
4. Wählen Sie in der Dropdown-Liste des Feldes **Kategorie** eine Kategorie für den Knoten auf Stammebene auf.

5. Wählen Sie in der Dropdown-Liste des Feldes **Symbol** den Dateinamen für das Symbol aus, das für den Knoten auf Stammebene stehen soll.
6. Klicken Sie auf **OK**, um den neuen Knoten links im Fenster **Beziehungen und Anzeige** hinzuzufügen.
7. Klicken Sie auf **Speichern**, um die Anzeige in den Portlets "Status" und "Key Performance Indicator - Drilldown" zu aktualisieren.

KPI-Legende ändern

Auf der Registerkarte **Beziehungen und Anzeige** können Sie die KPI-Legende im Portlet "Status" ändern.

Vorgehensweise

1. Klicken Sie links oben im Fenster **Beziehungen und Anzeige** auf **KPI-Legende**.
2. So ändern Sie die Anzeige der KPI-Legende:
   - Soll ein Bereich hinzugefügt werden, klicken Sie auf **Add Row** (Zeile hinzufügen).
   - Soll ein Bereich geändert werden, bearbeiten Sie die Felder unter **Range Name** (Bereichsname), **Color** (Farbe) und **Symbol**.
   - Soll ein Bereich gelöscht werden, klicken Sie auf **Löschen**.
3. Klicken Sie auf **OK**, um die Anzeige in den Portlets "Status" und "Key Performance Indicator - Drilldown" zu aktualisieren.

KPI-Modell anzeigen

Auf der Registerkarte **KPI-Definition** können Sie die KPIs anzeigen, die zu den KPI-Modellen in IBM Intelligent Operations Center gehören.

Vorgehensweise

Das Feld **Nach Modell filtern** enthält eine Dropdown-Liste mit Geschäftsprozessmodellen, zu deren Anzeige Sie berechtigt sind. Wählen Sie alle Modelle bzw. das Modell aus, deren bzw. dessen KPIs angezeigt werden sollen. Die KPI-Informationen werden wie in der folgenden Tabelle beschrieben angezeigt:

Option	Bezeichnung
KPI-Name	Titel des KPI. Durch Klicken auf den KPI-Namen werden die Eigenschaften angezeigt.
Modell	Name des Modells, zu dem der KPI gehört.
Erstellt	Methode zur Erstellung des KPI: • Ein modellierter KPI wurde mithilfe von IBM WebSphere Business Monitor auf Modellebene erstellt. • Ein Dashboard-KPI wurde mithilfe des Portlets "Key Performance Indicators (KPIs)" erstellt.
Typ	Typ des KPI: • Ein Aggregat-KPI hat einen Wert, der auf der von Ihnen ausgewählten Messgröße und Aggregationsmethode basiert. • Ein Ausdrucks-KPI hat einen Wert, der (unter Verwendung eines von Ihnen definierten XPath-Ausdrucks) auf anderen KPIs oder benutzerdefinierten Funktionen basiert.
Zugriff	Zugriffsebene eines KPI: • Ein gemeinsam genutzter KPI kann auch von anderen Benutzern angezeigt werden. • Ein privater KPI wird nur vom Eigner und nicht zusätzlich von anderen Benutzern genutzt.

KPI anzeigen oder ändern

Auf der Registerkarte **KPI-Definition** können Sie einen KPI, der zu einem Modell in IBM Intelligent Operations Center gehört, anzeigen oder ändern.

Vorgehensweise

1. Wählen Sie einen KPI aus. Klicken Sie links oben im Fenster **KPI-Definition** auf **Bearbeiten**. Das Fenster mit den KPI-Eigenschaften wird geöffnet.
2. Um den KPI zu ändern, bearbeiten Sie die Felder auf den Registerkarten des Eigenschaftenfensters. Weitere Details zum Bearbeiten dieser Felder, um einen Aggregat- oder Ausdrucks-KPI zu erstellen, erhalten Sie, indem Sie auf den entsprechenden Link unten klicken.

   Anmerkung: Die Definition eines modellierten KPI kann hier nicht geändert werden.
3. Um die Änderungen im Fenster mit den KPI-Eigenschaften zu speichern und das Fenster zu schließen, klicken Sie auf **OK**. Um die bisher gemachten Änderungen zu speichern und weitere Änderungen an dem kopierten KPI vorzunehmen, klicken Sie auf **Anwenden**. Um das Fenster zu schließen, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

KPI kopieren

Auf der Registerkarte **KPI-Definition** können Sie eine Kopie eines vorhandenen KPI für ein Modell in IBM Intelligent Operations Center erstellen.

Vorgehensweise

1. Wählen Sie einen KPI aus und klicken Sie links oben im Fenster **KPI-Definition** auf **Weitere Aktionen** > **Copy** (Kopieren). Das Fenster mit den KPI-Eigenschaften wird geöffnet.
2. Geben Sie im Feld zum KPI-Namen einen neuen Namen für den KPI ein.
3. Bearbeiten Sie die Eigenschaften des kopierten KPI wie unter Schritt 3 und 4 in den Hinweisen zum Ändern von KPIs beschrieben.

KPI erstellen

Auf der Registerkarte **KPI-Definition** können Sie einen KPI für ein Modell in IBM Intelligent Operations Center erstellen.

Vorgehensweise

1. Klicken Sie links oben im Fenster **KPI-Definition** auf **Erstellen**.
2. Klicken Sie auf **New Aggregate KPI** (Neuer Aggregat-KPI) oder **New Expression KPI** (Neuer Ausdrucks-KPI). Das Fenster mit den KPI-Eigenschaften wird geöffnet.
3. Bearbeiten Sie die Eigenschaften des neuen KPI wie unter Schritt 3 und 4 in den Hinweisen zum Ändern von KPIs beschrieben.

Nächste Schritte

Weitere Informationen zum Erstellen von KPIs erhalten Sie über den Link zur IBM Websphere Business Monitor-Dokumentation am Ende des Themas.

Beispiel-KPIs

In der Lösung stehen mehrere Beispiel-KPIs bereit. Diese KPIs sollen bei der Planung und Implementierung verschiedener, für Ihre Einrichtung relevanter KPIs helfen. Es werden Beispiele aus dem Bereich Wasser, Transport und öffentliche Sicherheit bereitgestellt.

Portlet "Key Performance Indicators (KPIs)" anpassen

Sie haben die Möglichkeit, dieses Portlet anzupassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Zugehörige Konzepte:

„Status" auf Seite 306
Mit dem Portlet "Status" können Sie den Status von KPIs einer einzelnen Einrichtung oder mehrerer Einrichtungen anzeigen.

„Key Performance Indicator - Drilldown" auf Seite 290
Mit dem Portlet "Key Performance Indicator - Drilldown" können Sie weitere Informationen zu einer KPI-Kategorie, den Status der untergeordneten KPIs anzeigen.

Zugehörige Verweise:

„Einstellungen des Key Performance Indicators (KPIs)-Portlets" auf Seite 163
Anpassen des Key Performance Indicators (KPIs)-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Zugehörige Informationen:

Information Center für IBM WebSphere Business Process Management Version 7.0

Vor der Anpassung von KPIs Sicherung durchführen

Sichern und stellen Sie KPIs wieder her, die mit IBM WebSphere Business Monitor oder mit dem Portlet "Key Performance Indicators (KPIs)" erstellt oder geändert wurden.

Informationen zu diesem Vorgang

Bevor Sie KPI-Modelle anpassen und KPIs ändern, möchten Sie möglicherweise bestehende Modelle sichern. Die Prozedur in diesem Thema exportiert alle KPIs aus dem angegebenen Modell in die angegebene Datei und importiert KPIs aus der angegebenen Datei in das angegebene Modell.

Vorgehensweise

1. Melden Sie sich beim Anwendungsserver an.
2. Wechseln Sie in das Verzeichnis `bin` des IBM WebSphere Business Monitor-Profils: `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin`
3. Führen Sie zum Exportieren von KPIs folgenden Befehl aus: `./wsadmin.sh -wsadmin_classpath "../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../scripts.wbm/kpi/exportKpis.jy" "`*`XML-Dateipfad`*`" `*`Modell-ID Modellversion`* `ALL`

   XML-Dateipfad ist der Name und der Pfad der XML-Datei, in die Sie KPIs exportieren. *Modell-ID* und *Modellversion* sind die ID und die Version des KPI-Modells, aus der Sie KPIs exportieren.
4. Führen Sie zum Importieren von KPIs folgenden Befehl aus: `./wsadmin.sh -wsadmin_classpath "../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../scripts.wbm/kpi/importKpis.jy" "`*`XML-Dateipfad`*`"`

   XML-Dateipfad ist der Name und der Pfad der XML-Datei, aus der Sie KPIs importieren.

Beispiel

Führen Sie den folgenden Befehl aus, um alle KPIs aus dem Modell `icoc_sample_public_safety_monitor_model` in `/tmp/kpis.xml` zu exportieren. In dem Befehl hat *XML-Dateipfad* den Wert `/tmp/kpis.xml`, *Modell-ID* den Wert `icoc_sample_public_safety_monitor_model` und *Modellversion* den Wert `2011-02-18T10:49:46`.

```
./wsadmin.sh -wsadmin_classpath "../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:
../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../scripts.wbm
/kpi/exportKpis.jy" "/tmp/kpis.xml" icoc_sample_public_safety_monitor_model
2011-02-18T10:49:46 ALL
```

Weitere Informationen erhalten Sie über den Link zum Information Center für WebSphere Business am Ende des Themas.

Zugehörige Verweise:

„Daten sichern” auf Seite 273
Um den Verlust von geschäftskritischen Daten in IBM Intelligent Operations Center zu vermeiden, sichern Sie bestimmte Dateien, Verzeichnisse und Datenbanken in regelmäßigen Zeitabständen.

Zugehörige Informationen:

Redbooks für IBM Smarter Cities Software Solutions

Ereigniskorrelation anpassen

Dieser Abschnitt enthält Erläuterungen zur Ereigniskorrelation und beschreibt, wie neue Entscheidungstabellen geändert und erstellt werden. Darüber hinaus wird die Regelanwendung beschrieben.

Ereigniskorrelation und Regelanwendung

Dieses Thema enthält eine Übersicht zum Ereigniskorrelationsprozess und eine kurze Erläuterung der Regelanwendung.

Mit der Anwendung für Ereigniskorrelationsregeln in WebSphere Operational Decision Management können Sie Korrelationsregeln ohne fundierte technische Kenntnisse von IBM Intelligent Operations Center oder WebSphere Operational Decision Management ändern und erweitern. Grundkenntnisse über Common Alerting Protocol-Ereignisse und WebSphere Operational Decision Management sind jedoch erforderlich.

Drei Variablen bestimmen, wie Ereignisse korrelieren: das Quellereignis, das Zielereignis und die Entscheidungstabelle.

Für jedes eingehende Common Alerting Protocol-Ereignis wird die Regelanwendung aufgerufen, um zu bestimmen, ob bestehende Ereignisse mit dem eingehenden Ereignis korrelieren. Das Quellereignis ist immer das neue eingehende Ereignis und es löst die Korrelation aus. Der Korrelationsprozess prüft das Quellereignis anhand der Ereignisse in der Datenbank. Wenn ein Ereignis in der Datenbank gefunden wird, das mit dem Quellereignis korreliert, wird dieses Ereignis als Zielereignis bezeichnet. Jedes Mal, wenn eine mögliche Korrelation gefunden wird, sendet das Portlet "Benachrichtigungen" einen Alert.

Die Bestimmung ist unidirektional. Dieses Konzept ist wichtig, da die Regeln, die die Korrelation bestimmen, nicht symmetrisch sein müssen. Beispiel: Wenn Ereignis A mit Ereignis B korreliert, bedeutet dies nicht, dass Ereignis B mit Ereignis A korreliert.

Die Regelanwendung stellt eine Beispielkorrelationstabelle bereit, die den meisten Anforderungen entspricht. Unter „Einstellungen für Ereigniskorrelation anpassen” finden Sie verschiedene Methoden zur Anpassung der Korrelationsregeln.

Einstellungen für Ereigniskorrelation anpassen

In diesem Abschnitt wird die Vorgehensweise zur Anpassung von Ereigniskorrelationseinstellungen erläutert.

Die Entscheidungstabelle, die im Decision Center bearbeitet werden kann, enthält zwei Spaltentypen. Die Spalten links werden als Entscheidungsspalten bezeichnet. Sie bestimmen, welche Aktionsspalte auf der rechten Seite verwendet wird. Die Entscheidungstabellen werden von links nach rechts geprüft und führen, abhängig von den Werten der verschiedenen Zeilen, zu einer Aktionsspalte auf der rechten Seite. Die Aktionsspalte definiert, was ausgeführt wird, wenn eine bestimmte Zeile erreicht wird.

Zur Erweiterung und Änderung von Ereigniskorrelationseinstellungen wird empfohlen, eine bestehende Entscheidungstabelle zu bearbeiten. Die folgenden Elemente beschreiben, wie Entscheidungstabellen formatiert werden:

- Auf der linken Seite der Entscheidungstabelle (weißer Hintergrund) befinden sich die Entscheidungsspalten. Sie bestimmen, welche Zeilen in den Aktionsspalten (grauer Hintergrund) ausgeführt werden.
- Die letzte Aktionsspalte in der Tabelle ruft den Abfrage- und Veröffentlichungsservice auf. Wenn eine Aktionszeile vorhanden ist, die nicht als Korrelationsabfrage und -veröffentlichung verwendet werden soll, inaktivieren Sie den Eintrag in dieser letzten Spalte.
- Die Spalte zum Setzen einer SQL-Abfrage in den Aktionsspalten kann die Abfrageparameter überschreiben. Das Überschreiben von Abfrageparametern ist umständlich und für die meisten Anwendungen überflüssig. Die Anforderung für diese Abfrage ist, dass drei benannte Spalten im Abfrageergebnis vorhanden sind:
  - event_headline - Der in der Beschreibung der Korrelation zu verwendende Titel. Dieser Text wird als Benachrichtigungsbeschreibung verwendet.
  - event_external_id - Die externe ID, wie z. B. CAP-ID, des Ereignisses
  - event_internal_id - Die interne ID, wie z. B. CapAlertId, die vom Portlet "Benachrichtigungen" Überschriften im Feld **Refers to Alerts** (Bezieht sich auf Alerts) den Benachrichtigungseigenschaften zugeordnet wird.

Dieser Abschnitt enthält die folgenden Themen:

Entscheidungseigenschaften ändern

Verwenden Sie die Decision Center-Benutzerschnittstelle in WebSphere Operational Decision Management, um Einstellungen für die Ereigniskorrelation zu ändern. In diesem Thema sind weiterführende Informationen zum Ändern der Entscheidungseigenschaften in den Entscheidungstabellen enthalten. Darüber hinaus ist ein Link zur Dokumentation für WebSphere Operational Decision Management enthalten.

Informationen zu diesem Vorgang

Die Benutzerschnittstelle befindet sich auf Knoten 1 der Installation von Portalserver unter dieser URL: http://*Anwendungsserver*:9084/teamserver. Melden Sie sich als `waswebadmin` an.

Die meisten Änderungen können innerhalb der Regelanwendung wie in „Entscheidungstabelle bearbeiten” beschrieben vorgenommen werden. Andere Änderungen beinhalten möglicherweise Änderungen an Folgendem:

- Die Tivoli Netcool/Impact-Richtlinien
- Der Java-Rechenknoten von WebSphere Message Broker, der die Nachrichten aus den Auswirkungsrichtlinien in das nachrichtengesteuerte Beanformat umwandelt.
- Das Execution Object Model (XOM) der Abfrage und das Geschäftsobjektmodell (BOM; Business Object Model)

Weitere Informationen und Anweisungen zum Ändern des XOM und des BOM, Informationen zum Nachrichtenbrokerknoten und Informationen zum Decision Center finden Sie im jeweiligen Information Center für WebSphere Operational Decision Management undWebSphere Message Broker, wenn Sie auf die folgenden Links klicken.

Zugehörige Informationen:

Information Center für IBM WebSphere Operational Decision Management

WebSphere Message Broker-Dokumentation

Entscheidungstabelle bearbeiten

Dieses Thema enthält eine kurze Erläuterung zur Entscheidungstabelle und stellt Schritte zum Ändern der Eigenschaften der Entscheidungstabelle bereit.

In der IBM Intelligent Operations Center WebSphere Operational Decision Management-Regelanwendung ist eine Basiskorrelationstabelle definiert, die die Kategorie und den Typ des Ereignisses verwendet, um die auszuführende Aktionszeile zu bestimmen.

Die Aktionszeilen sind derzeit identisch, können jedoch Ihren Anforderungen entsprechend geändert werden. Beispiel: Sie können definieren, dass Brandereignisse anders als andere Ereignisse behandelt werden und nur mit Wasserereignissen und anderen Brandereignissen korrelieren. Um Werte Ihren Anforderungen entsprechend zu ändern, aktivieren Sie die Spaltenzelle "Categories" (Kategorien) für die Zeile und geben Sie "Fire, Water" in der Zelle ein. Wenn die Regel zwischen Ereignissen und Vorfällen unterscheiden soll, fügen Sie dieser Entscheidungsspalte und der Aktionsspalte eine Zeile hinzu.

Um den Suchradius für korrelierende Ereignisse zu ändern, ändern Sie den Wert **Set search radius** (Suchradius festlegen). Die eingegebene Ganzzahl wird als Abstand (in Metern) vom Zentrum des Quellereignisses interpretiert. Wenn Sie also `2000` eingeben, korreliert es nur mit Ereignissen, deren Abstand vom Quellereignis weniger als 2000 Meter beträgt.

Eigenschaften der Entscheidungstabelle ändern

Vorgehensweise

1. Melden Sie sich als `rtsadmin` bei http://*Anwendungsserver*:9084/teamserver an.
2. Wechseln Sie zum Explorer Ihres Browsers.
3. Klicken Sie auf **capCorrelationRules**.
4. Klicken Sie auf **simpleCorrelationPolicy**.
5. Klicken Sie auf **Bearbeiten**. Die Eigenschaftenseite wird angezeigt.
6. Klicken Sie auf der Eigenschaftenseite auf **Weiter**.
7. Bearbeiten Sie die Tabelle. Beispiele für Spalten, die Sie der Entscheidungstabelle hinzufügen können, finden Sie in der im Vorlagenordner enthaltenen Vorlage.
8. Wenn Sie alle Änderungen an den Eigenschaften vorgenommen haben, klicken Sie auf **Finish** (Fertig stellen).

Nächste Schritte

Exportieren Sie die Regelanwendung aus dem Decision Center über den im Folgenden angegebenen zugehörigen Link.

Zugehörige Tasks:

„Geänderten Regelsatz im IBM Intelligent Operations Center-Fluss implementieren”
Verwenden Sie dieses Thema, um den geänderten Regelsatz auf dem Regelausführungsserver zu implementieren.

Geänderten Regelsatz im IBM Intelligent Operations Center-Fluss implementieren

Verwenden Sie dieses Thema, um den geänderten Regelsatz auf dem Regelausführungsserver zu implementieren.

Informationen zu diesem Vorgang

Wenn Sie Eigenschaften oder Elemente in der Entscheidungstabelle ändern, müssen Sie den geänderten Regelsatz im Ereignisfluss im IBM Intelligent Operations Center implementieren. Nach der Implementierung des geänderten Regelsatzes auf dem Regelausführungsserver haben die Korrelationsregeln je nach Änderung andere Funktionen. Der Regelausführungsserver prüft die eingehenden Ereignisse auf mögliche Korrelationen.

Gehen Sie wie folgt vor, um den geänderten Regelsatz zu implementieren.

Vorgehensweise

1. Exportieren Sie die Regelanwendung aus dem Decision Center:
   a. Wechseln Sie zu *Anwendungsserver*:9084/teamserver/.
   b. Melden Sie sich bei rtsadmin an.
   c. Navigieren Sie zu **Project** > **Generate RuleSet** (Projekt > Regelsatz generieren).
   d. Klicken Sie auf **Weiter**, wählen Sie nichts aus und laden Sie die JAR-Datei "RuleApp" herunter.
2. Importieren Sie die Regelanwendung auf dem Regelausführungsserver:
   a. Gehen Sie zu *Anwendungsserver*:9083/res.
   b. Klicken Sie auf die Registerkarte "Explorer".
   c. Klicken Sie auf **icoc_wodm_correlation_ruleApp** > **Add Ruleset** (Regelsatz hinzufügen).
   d. Benennen Sie den Regelsatz und notieren Sie sich den Pfad des neuen Regelsatzes: /icoc_wodm_correlation_ruleApp/1.0/*Ihr_ausgewählter_Name*/*Version*.
      Dabei ist
      - *Ihr_ausgewählter_Name* der Name, den Sie für den Regelsatz auswählen
      - *Version* die Version des Regelsatzes
3. Legen Sie den neuen Pfad des Regelsatzes in der Auswirkungsrichtlinie fest:
   a. Wechseln Sie zu Ereignisserver:9080/nci/*login_main*.jsp.
   b. Wählen Sie im Dropdown-Menü links die Option IBM Intelligent Operations Center aus.
   c. Klicken Sie auf **Richtlinien** und wählen Sie die Richtlinie **IOC_Event_Correlation** aus.
   d. Ändern Sie den Wert des Felds **JMSProps.ilog_rules_bres_mdb_rulesetPath** in den neuen Pfad: /icoc_wodm_correlation_ruleApp/1.0/*Ihr_ausgewählter_Name*/*Version*.
      Dabei ist
      - *Ihr_ausgewählter_Name* der Name, den Sie für den Regelsatz ausgewählt haben
      - *Version* die Version des Regelsatzes
   e. Klicken Sie auf **Speichern**.

Zugehörige Tasks:

„Eigenschaften der Entscheidungstabelle ändern” auf Seite 185

Positionskartenmanager

Mithilfe des Portlets "Positionskartenmanager" können Sie das Portlet "Positionskarte" anpassen.

Folgendes kann im Portlet "Positionskarte" angepasst werden:

- Der Klassifikationsname, der im Menü links im Portlet angezeigt werden soll.
- Die Karte, die im Portlet angezeigt werden soll.
- Die Bereiche in einer Karte.

Bereiche in einer Karte werden über einen Bereichs-ID-Code bestimmt. Alle Ereignisse mit einem Bereichs-ID-Code werden in allen Positionskarten mit dem definierten Bereich angezeigt.

Es besteht auch die Möglichkeit, einem Bereich eine übergeordnete ID zuzuordnen. Mithilfe der übergeordneten ID können Sie eine Bereichshierarchie erstellen. Erstellen Sie z. B. Bereiche, um die Sitzplatzbereiche auf der ersten Ebene eines Sportstadiums darzustellen. Dabei wird jeder Sitzplatzbereich in der detaillierten Positionskarte der ersten Ebene des Sportstadiums definiert. Vergeben Sie zusätzlich eine übergeordnete ID an die einzelnen Sitzplatzbereiche, um zu kennzeichnen, dass diese sich auf der ersten Ebene des Stadiums befinden. Daraufhin wird ein Ereignis mit einer Bereichs-ID für einen der Sitzplatzbereiche auf der ersten Ebene in der detaillierten Karte angezeigt. Zudem erscheint dieses Ereignis in einer Übersichtskarte des Stadiums, da die hier verwendete Bereichs-ID für die erste Ebene identisch ist mit der übergeordneten ID für die Sitzplatzbereiche.

Um auf das Portlet "Positionskartenmanager" zuzugreifen, klicken Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Customization Tools** > **Location Map Manager** (Intelligent Operations > Anpassungstools > Positionskartenmanager).

Klassifikation im Kartenmenü hinzufügen

Über die Registerkarte **Klassifikationen** können Sie eine Klassifikation hinzufügen, die im Kartenmenü des Portlets "Positionskarte" angezeigt werden soll.

Vorgehensweise

1. Geben Sie im Feld **Klassifikationsname** einen Namen ein. Sie haben die Möglichkeit, eine Beschreibung hinzuzufügen.
2. Klicken Sie auf **Senden**, um die Klassifikation dem Portlet hinzuzufügen.

Ergebnisse

Die neue Klassifikation wird im Portlet "Positionskarte" nach einer Aktualisierung der Portletseite angezeigt.

Karte im Portlet hinzufügen

Über die Registerkarte **Positionskarten** können Sie eine Positionskarte hinzufügen, die im Portlet "Positionskarte" angezeigt werden soll.

Vorgehensweise

1. Geben Sie im Feld **Klassifikationsname** einen Namen ein. Sie können in der Dropdown-Liste einen Namen auswählen.
2. Geben Sie im Feld **Name der Karte** einen Positionsnamen ein. Sie haben die Möglichkeit, eine Beschreibung der Karte hinzuzufügen.
3. Geben Sie eine URL für die Positionskarte im Feld für das Bild ein.
4. Klicken Sie auf **Senden**, um die Karte dem Portlet hinzuzufügen.

Ergebnisse

Die Karte wird im Portletmenü "Positionskarte" nach einer Aktualisierung der Portletseite angezeigt. Sie können anschließend die Karte auswählen und anzeigen.

Bereiche in einer Positionskarte hinzufügen oder ändern

Über die Registerkarte **Bereiche** können Sie neue Bereiche erstellen sowie Bereiche ändern oder entfernen, sodass sie nicht mehr in einer Positionskarte im Portlet "Positionskarte" angezeigt werden.

Vorgehensweise

1. Geben Sie im Feld **Name der Karte** einen Kartennamen ein. Sie können unter den Karten in der Dropdown-Liste auswählen.
2. Soll ein neuer Bereich in der Karte gezeichnet werden, klicken Sie rechts oben im Fenster auf das Polygonsymbol. Klicken Sie auf die gewünschte Position in der Karte und anschließend auf die einzelnen Ecken, um ein Polygon zu zeichnen. Klicken Sie anschließend doppelt, um das Polygon fertigzustellen. Die neuen Bereiche werden standardmäßig grün angezeigt.
3. Sie können Details für einen Bereich eingeben, indem Sie oben rechts im Fenster auf das Handsymbol klicken. Klicken Sie auf den Bereich, um ihn zu aktualisieren.
4. Geben Sie im Feld **Name des Bereichs** einen Namen ein. Sie haben die Möglichkeit, eine Beschreibung hinzuzufügen.
5. Geben Sie im Feld **Bereichs-ID** eine Kennung für den Bereich ein. Sie haben die Möglichkeit, eine übergeordnete Bereichs-ID hinzuzufügen.

6. Um einen Bereich zu aktualisieren, klicken Sie auf **Bereich aktualisieren**. Um einen Bereich zu entfernen, klicken Sie auf **Bereich entfernen**.
7. Um Ihre Änderungen für die Karte zu übernehmen, klicken Sie auf **Senden**.

Ergebnisse

Die Änderungen werden im Portlet "Positionskarte" nach einer Aktualisierung der Portletseite angezeigt.

Portlet "Positionskartenmanager" anpassen

Sie haben die Möglichkeit, dieses Portlet anzupassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Zugehörige Konzepte:

„Positionskarte" auf Seite 291
Mit dem Portlet "Positionskarte" können Sie die auf einer Positionskarte markierten Ereignisse anzeigen. Eine Positionskarte im IBM Intelligent Operations Center ist eine Karte oder ein Plan mit vordefinierten Interaktionsbereichen, wie z. B. Sitzbereiche in großen Sportstadien.

Zugehörige Verweise:

„Einstellungen des Positionskartenmanager-Portlets" auf Seite 165
Anpassen des Positionskartenmanager-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Systemweite Konfigurationsdaten angeben

In der Tabelle mit den Systemeigenschaften von IBM Intelligent Operations Center sind IBM Intelligent Operations Center-Konfigurationsdaten gespeichert.

Die folgenden Eigenschaften sind systemweite Eigenschaften, die vom IBM Intelligent Operations Center verwendet werden.

Tabelle 63. Systemweite Werte, die vom IBM Intelligent Operations Center verwendet werden

Bereich	Thema	Name	Typ	Wert
System	*	ActivityCollectionRefreshInterval	Ganzzahl	Die Aktualisierungsrate der Sammlung auf dem Server in Sekunden. Der Standardwert ist 300 (5 Minuten). Diese Eigenschaft wirkt sich auf die Servicerate der Benutzerschnittstelle für Aktualisierungen von Aktivitäten aus.
System	*	ActivityProviderEJBJNDIName	Zeichenfolge	Der JNDI-Bindungsname der fernen Schnittstelle des Aktivitätsproviders. Mit dieser Schnittstelle können Sie Ihren eigenen Aktivitätsprovider für die Arbeit mit Ihrem Prozess- oder Workflow-Management-System implementieren. Der Aktivitätsprovider ist eine EJB, die die Aktivitätsschnittstelle in iss_common.jar implementiert.
System	*	AppMonitorPort	Zeichenfolge	Der Web-Port, der von Tivoli Monitoring verwendet wird.
System	*	ApplicationServerHostname	Zeichenfolge	Der Hostname oder die IP-Adresse, der bzw. die vom Anwendungsserver verwendet wird.

Tabelle 63. Systemweite Werte, die vom IBM Intelligent Operations Center verwendet werden (Forts.)

Bereich	Thema	Name	Typ	Wert
System	*	CollectionRefreshInterval	Ganzzahl	Die Aktualisierungsrate der Sammlung auf dem Server in Sekunden. Der Standardwert ist 15 Sekunden.Diese Eigenschaft wirkt sich auf die Servicerate der Benutzerschnittstelle für Aktualisierungen von Aktivitäten und Benachrichtigungen aus.
System	*	DatabaseServerHostname	Zeichenfolge	Der Hostname oder die IP-Adresse, der bzw. die vom Datenserver verwendet wird.
System	*	DateFormat	Zeichenfolge	Das Format, das verwendet wird, wenn das IBM Intelligent Operations Center das Datum anzeigt. Der Standardwert ist `yyyy-MM-dd`. Jedes beliebige gültige Java `java.text.SimpleDateFormat`-Datumsmuster kann angegeben werden.
System	*	DateTimeFormat	Zeichenfolge	Das Format, das verwendet wird, wenn das IBM Intelligent Operations Center das Datum und die Uhrzeit anzeigt. Der Standardwert ist `yyyy-MM-dd HH:mm:ss`. Jedes beliebige gültige Java `java.text.SimpleDateFormat`-Muster für Datum und Uhrzeit kann angegeben werden.
System	*	DisableTSRMSync	Boolesch	Gibt an, ob die Tivoli Service Request Manager-Synchronisation inaktiviert ist. Der Standardwert ist "false". Auf "true" gesetzt, wenn die Tivoli Service Request Manager-Installation in einer Implementierung nicht enthalten ist.
System	*	EventContainerDeleteEvent	Zeichenfolge	Gibt an, ob ein Ereignis aus der Objektserverdatenbank von Tivoli Netcool/OMNIbus gelöscht wird. Der Löschvorgang wird von der Tivoli Netcool/Impact-Richtlinie implementiert, wenn die IBM Intelligent Operations Center-Datenbank mit einem Ereignis aktualisiert wird. Der Standardwert ist `true`. Wenn der Wert auf `true` gesetzt ist, wird das Ereignis aus der Objektserverdatenbank gelöscht. Wenn der Wert auf `false` gesetzt ist, wird das Ereignis nicht aus der Objektserverdatenbank gelöscht.
System	*	EventRouterPollDelay	Ganzzahl	Die Verzögerung in Millisekunden zwischen Abfrageintervallen der Benutzerschnittstelle. Die Verzögerung ist die Wartezeit in Millisekunden bis zum nächsten Abfrageintervall. Der Standardwert ist `0`.

Tabelle 63. Systemweite Werte, die vom IBM Intelligent Operations Center verwendet werden (Forts.)

Bereich	Thema	Name	Typ	Wert
System	*	EventRouterPollErrorDelay	Ganzzahl	Die Verzögerung in Millisekunden zwischen Abfrageintervallen der Benutzerschnittstelle bei einem Fehler. Die Verzögerung ist die Wartezeit nach einem Fehler (in Millisekunden) bis zum nächsten Abfrageintervall. Der Standardwert ist `5000`.
System	*	EventRouterTimeout	Ganzzahl	Das Abfrageintervall der Benutzerschnittstelle in Sekunden. Das Abfrageintervall ist das Zeitintervall, in dem Ereignisse vor Ablauf eines Zeitlimits abgefragt werden. Der Standardwert ist `20`.
System	*	EventServerHostname	Zeichenfolge	Der Hostname oder die IP-Adresse, der bzw. die vom Ereignisserver verwendet wird.
System	*	MgmtServerHostname	Zeichenfolge	Der Hostname oder die IP-Adresse, der bzw. die vom Verwaltungsserver verwendet wird.
System	*	ModelManagerServerEJBPort	Zeichenfolge	Der EJB-Port, der von Semantic Model Services verwendet wird.
System	*	ModelManagerServerHostname	Zeichenfolge	Der Hostname oder die IP-Adresse, der bzw. die von Semantic Model Services verwendet wird.
System	*	MonitorServerHostname	Zeichenfolge	Der Hostname oder die IP-Adresse, der bzw. die von IBM WebSphere Business Monitor verwendet wird.
System	*	MonitorServerWebPort	Zeichenfolge	Der Web-Port, der vom Gateway für die IBM WebSphere Business Monitor-REST-Services verwendet wird.
System	*	MonitorServerSecurityEnabled	Boolesch	Gibt an, ob die Verbindung zu IBM WebSphere Business Monitor SSL für eine sichere HTTP-Verbindung verwendet. Der Standardwert ist `true`. Wenn der Wert auf `true` gesetzt ist, verwendet die Verbindung SSL. Wenn der Wert auf `false` gesetzt ist, verwendet die Verbindung kein SSL.
System	*	PortalServerHostname	Zeichenfolge	Der Hostname oder die IP-Adresse, der bzw. die von WebSphere Portal Server verwendet wird.
System	*	PortalServerWebPort	Zeichenfolge	Der Web-Port, der vom WebSphere Portal Server verwendet wird.
System	*	RegExpEmail	System	Der reguläre Ausdruck, der zum Prüfen einer E-Mail-Adresse verwendet wird. Der Standardwert ist `.+`.
System	*	RegExpTelephone	System	Der reguläre Ausdruck, der zum Prüfen einer Telefonnummer verwendet wird. Der Standardwert ist `.+`

Tabelle 63. Systemweite Werte, die vom IBM Intelligent Operations Center verwendet werden (Forts.)

Bereich	Thema	Name	Typ	Wert
System	*	SecurityUserPrefix	Zeichenfolge	Das Präfix der Benutzer-ID, das verwendet wird, um den Benutzer dem definierten LDAP-Namen zuzuordnen. Der Standardwert ist `uid`.
System	*	SecurityUserSuffix	Zeichenfolge	Das Suffix der Benutzer-ID, das verwendet wird, um dem Benutzer einen definierten LDAP-Namen oder einen lokalen definierten Namen zuzuordnen. Der Standardwert, der bei der Ausführung eines Portals mit LDAP-Sicherheit verwendet wird, ist `ou=users,ou=SWG,o=IBM,c=US`. Setzen Sie den Wert auf `o=defaultWIMFileBasedRealm`, wenn Sie ein lokales Portal ohne LDAP-Sicherheit ausführen.
System	*	TdsPort	Zeichenfolge	Der Web-Port, der von Tivoli Directory Server Web Administration Tool verwendet wird
System	*	TimeFormat	Zeichenfolge	Das Format, das verwendet wird, wenn das IBM Intelligent Operations Center die Uhrzeit anzeigt. Der Standardwert ist `HH:mm:ss`. Jedes beliebige gültige Java `java.text.SimpleDateFormat`-Zeitmuster kann angegeben werden.
System	*	TSRMDirectServerHostname	Zeichenfolge	Der Hostname oder die IP-Adresse, der bzw. die vom Tivoli Service Request Manager verwendet wird.
System	*	TSRMDirectServerWebPort	Zeichenfolge	Der Web-Port, der von Tivoli Service Request Manager verwendet wird.
System	*	TSRMServerActivityUri	Zeichenfolge	Die Aktivitäts- und Taskanwendungs-URI, die von Tivoli Service Request Manager verwendet wird. Der Standardwert ist `/tsrm/maximo/ui/maximo?event=loadapp &value=Activity&uniqueid={0}`. Der Wert für die Aktivitäts-ID wird durch `{0}` ersetzt.
System	*	TSRMServerResourceAddUri		Die URI zum Hinzufügen von Ressourcen, die von Tivoli Service Request Manager verwendet wird. Der Standardwert ist `/tsrm/maximo/ui/maximo?event=loadapp &value=plusires&additionalevent=INSERT`. Der Wert für die externe Ressourcen-ID wird durch `{0}` ersetzt.
System	*	TSRMServerResourceDeleteUri		Die URI zum Löschen von Ressourcen, die von Tivoli Service Request Manager verwendet wird. Der Standardwert ist `/tsrm/ maximo/ui/maximo?event=loadapp &value=plusires&additionalevent=useqbe &additionaleventvalue=LOCATION={0}`. Der Wert für die externe Ressourcen-ID wird durch `{0}` ersetzt.

Tabelle 63. Systemweite Werte, die vom IBM Intelligent Operations Center verwendet werden (Forts.)

Bereich	Thema	Name	Typ	Wert
System	*	TSRMServerResourcePropertiesUri		Die Ressourceneigenschaften-URI, die von Tivoli Service Request Manager verwendet wird. Der Standardwert ist `/tsrm/maximo/ui/maximo?event=loadapp&value=plusires &additionalevent=useqbe &additionaleventvalue=LOCATION={0}`. Der Wert für die externe Ressourcen-ID wird durch `{0}` ersetzt.
System	*	TSRMServerResourceUpdateUri		Die URI zum Aktualisieren von Ressourcen, die von Tivoli Service Request Manager verwendet wird. Der Standardwert ist `/tsrm/maximo/ui/maximo?event=loadapp &value=plusires&additionalevent=useqbe &additionaleventvalue=LOCATION={0}`. Der Wert für die externe Ressourcen-ID wird durch `{0}` ersetzt.
System	*	TSRMServerSecurityEnabled	Boolesch	Gibt an, ob die HTTP-Verbindung zu Tivoli Service Request Manager SSL verwendet. Der Standardwert ist `false`. Wenn der Wert auf `true` gesetzt ist, verwendet die Verbindung SSL. Wenn der Wert auf `false` gesetzt ist, verwendet die Verbindung kein SSL.
System	*	TSRMServerWorkflowUri	Zeichenfolge	Die Workflow-URI, die von Tivoli Service Request Manager verwendet wird. Der Standardwert ist `/maximo/ui/ ?event=loadapp&value=sr &&additionalevent=useqbe &additionaleventvalue=TICKETID={0}`. Der Wert für die Vorfall-ID wird durch `{0}` ersetzt.
System	*	UseDBModelReader	Boolesch	Gibt an, ob das KPI-Datenbankmodell aus einer RDF-Datei gelesen wird. Der Standardwert ist `true`. Wenn der Wert auf `true` gesetzt ist, wird das KPI-Modell nicht aus einer RDF-Datei gelesen. Wenn der Wert auf `false` gesetzt ist, wird das KPI-Modell aus einer RDF-Datei gelesen.
System	*	WebSEALServerHostname	Zeichenfolge	Der Hostname oder die IP-Adresse, der bzw. die von Tivoli Access Manager WebSEAL verwendet wird.

Die folgenden Eigenschaften können geändert werden, um die Verarbeitung von KPIs zu konfigurieren.

Tabelle 64. Eigenschaften, die sich auf die KPI-Verarbeitung auswirken

Bereich	Thema	Name	Typ	Wert
KPI	*	CacheKpis	Boolesch	Gibt an, ob aus IBM WebSphere Business Monitor abgerufene KPIs zwischengespeichert werden. Der Standardwert ist `true`. Wenn die Eigenschaft auf `true` gesetzt ist, werden KPIs zur Wiederverwendung zwischengespeichert. Wie oft der Cache aktualisiert wird, wird über `KpiCacheRefreshInterval` angegeben. Wenn der Wert auf `false` gesetzt ist, werden KPIs immer aus IBM WebSphere Business Monitor abgerufen, wenn das IBM Intelligent Operations Center KPI-Informationen anfordert.
KPI	*	KpiCacheRefreshInterval	Ganzzahl	Gibt an, wie oft der KPI-Cache aktualisiert wird. Das Intervall wird in Sekunden angegeben. Der Standardwert ist `300` (5 Minuten). `KPICacheRefreshInterval` wird ignoriert, wenn `CacheKpis` auf `false` gesetzt ist.
KPI	*	KpiSentToGroup	Zeichenfolge	Gibt die Gruppen an, die KPI-Benachrichtigungen empfangen. Trennen Sie Gruppennamen durch einen Semikolon (;). Der Standardwert ist `CityWideExecutive;CityWideSupervisor`.
KPI	*	PreLoadKpis	Boolesch	Gibt an, ob die KPIs aus IBM WebSphere Business Monitor abgerufen werden, wenn das IBM Intelligent Operations Center gestartet wird. Der Standardwert ist `true`. Wenn der Wert auf `true` gesetzt ist, werden alle KPIs aus IBM WebSphere Business Monitor abgerufen, wenn das IBM Intelligent Operations Center gestartet wird. Die KPIs werden zur Wiederverwendung zwischengespeichert. `KpiCacheRefreshInterval` gibt an, wie oft der KPI-Cache aktualisiert wird. Wenn die Eigenschaft auf `false` gesetzt ist, werden KPIs aus IBM WebSphere Business Monitor nur dann abgerufen, wenn das IBM Intelligent Operations Center KPI-Informationen anfordert. **Anmerkung:** Wenn `PreLoadKpis` auf `true` gesetzt ist, wird unabhängig vom angegebenen Wert davon ausgegangen, dass `CacheKpis` den Wert `true` hat.

Tabelle mit den Systemeigenschaften aktualisieren

Um die systemweiten IBM Intelligent Operations Center-Konfigurationsdaten zu ändern, aktualisieren Sie die Tabelle mit den Systemeigenschaften.

Informationen zu diesem Vorgang

Verwenden Sie einen VNC-Client, um sich beim Datenbankserver von Datenserver anzumelden, und öffnen Sie ein Befehlsfenster. Geben Sie gemäß der folgenden Vorgehensweise Befehle in das Befehlsfenster ein.

Vorgehensweise

1. Melden Sie sich beim Datenserver als Root an
2. Um das DB2® Control Center zu öffnen, inaktivieren Sie vorübergehend die Zugriffssteuerung; geben Sie die Befehle ein:

```
xhost +
su - db2inst1
db2cc
```

3. Öffnen Sie im DB2 Control Center die Tabelle mit den Systemeigenschaften:
   a. Geben Sie zum Öffnen des DB2 Control Center den folgenden Befehl ein: `- db2cc`
   b. Klicken Sie im DB2 Control Center auf **Alle Datenbanken** > **IOCDB** > **Tabellen** > **SYSPROP**.
   c. Klicken Sie mit der rechten Maustaste auf die Tabelle **SYSPROP** und anschließend auf **Öffnen**.
   d. Ändern Sie das erforderliche Feld und klicken Sie auf **Festschreiben**
   e. Schließen Sie die Tabelle.
4. Schließen Sie das DB2 Control Center.
5. Um zurück zum Rootbenutzer zu wechseln, geben Sie den folgenden Befehl ein: **exit** .
6. Um die Zugriffssteuerung erneut zu aktivieren, geben Sie den folgenden Befehl ein: **xhost -**

   Anmerkung: Um die vorgenommenen Änderungen zu implementieren, müssen Sie den Portalserver neu starten. Sie können den Portalserver mit dem Script "IOCControl" neu starten. Informationen zum Starten der Services erhalten Sie über den Link am Ende dieses Themas.

Zugehörige Tasks:

„Services starten" auf Seite 206
Zum Starten von Services, die auf IBM Intelligent Operations Center-Servern ausgeführt werden, ist das Plattformsteuerungstool verfügbar.

IBM Cognos Business Intelligence für das Erstellen von Berichten konfigurieren

IBM Intelligent Operations Center stellt ein Subsystem zur Berichterstellung mit IBM Cognos Business Intelligence bereit, um Berichte zu erstellen und zu verwalten. Im Lieferumfang von IBM Intelligent Operations Center ist eine Berichtsseite enthalten, auf der bis zu sechs Berichte angezeigt werden können. Sie können auch eine Berichtsseite manuell erstellen und das Portletlayout anpassen.

Das Subsystem zur Berichterstellung wird auf dem Anwendungsserver installiert und verwendet ein analytisches Datenmodell.

Berichtsportlet erstellen

Verwenden Sie die Informationen in diesem Thema, um eine Berichtsportletseite zu erstellen, indem Sie ein vorhandenes Portlet mit der IBM Intelligent Operations Center-Konsole kopieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein bestehendes Portlet zu kopieren und die Eigenschaften festzulegen, um eine neue Berichtsseite zu erstellen.

Vorgehensweise

1. Melden Sie sich als Administrator beim IBM Intelligent Operations Center an.
2. Navigieren Sie zu **Administration** > **Portlet Management** > **Portlets**.
3. Geben Sie im Feld **Suche** `Berichte` ein und klicken Sie auf **Suchen**. Das Portletfenster "Berichte" wird angezeigt.
4. Klicken Sie neben dem zu kopierenden Portlet auf das Symbol **Portlet kopieren**. Das Fenster "Portlet kopieren" wird angezeigt.
5. Geben Sie als Namen des neuen Portlets `CognosReport` ein.
6. Klicken Sie auf **OK**. Das neue Portlet wird im Fenster "Portlets verwalten" angezeigt.
7. Navigieren Sie zu **Administration** > **Portalbenutzerschnittstelle** > **Seiten verwalten**.

8. Klicken Sie auf **Inhaltsroot** > **Citywide** und klicken Sie auf die Registerkarte **Neue Seite**. Die Seite "Seiteneigenschaften" wird angezeigt.
9. Geben Sie die folgenden Eigenschaften für die neue Berichtsseite ein:
   a. Geben Sie im Feld **Titel** einen Titel für die Berichtsseite ein. Ein Beispieltitel ist `Operator: Berichte`.
   b. Geben Sie im Feld **Eindeutiger Name** einen Namen ein, der diese Berichtsseite speziell bestimmt. Ein Beispiel für einen eindeutigen Namen ist `com.ibm.iss.ioc.citywide.OperatorReports`.
   c. Geben Sie im Feld **Optimierter URL-Name** `report` ein.
   d. Akzeptieren Sie im Feld **Motiv** den Standardwert **Übergeordnetes Motiv übernehmen**.
   e. Akzeptieren Sie im Feld **Motivstil** den Standardwert **Übergeordnete Motivrichtlinie übernehmen**.
   f. Wählen Sie unter **Aggregation-Render Mode** (Aggregations-Wiedergabemodus) den Standardwert **Inherit Parent Render Mode** (Übergeordneten Wiedergabemodus übernehmen) aus.
   g. Klicken Sie auf **OK**.

   Die neue Berichtsseite wird der Liste der Portletseiten hinzugefügt.

Das Layout des Portlets "Berichte" bearbeiten

Mit diesen Schritten können Sie das Layout der Portletseite "Berichte" formatieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um das Layout der Portletseite "Berichte" mit der IBM Intelligent Operations Center-Konsole auszuwählen.

Vorgehensweise

1. Melden Sie sich als Administrator beim IBM Intelligent Operations Center an.
2. Navigieren Sie zu **Administration** > **Portalbenutzerschnittstelle** > **Seiten verwalten**.
3. Klicken Sie neben der zu editierenden Seite auf das Symbol **Seitenlayout bearbeiten**. Die Seite "Layout bearbeiten" wird angezeigt.
4. Wählen Sie das Layoutsymbol aus, das über parallele Seiten mit einer Zeile unter den Seiten verfügt. Dieses Symbol ist das fünfte Symbol von links.
5. Klicken Sie im Frame, in dem Sie das Portlet hinzufügen möchten, auf **Portlets hinzufügen**.
6. Suchen Sie das Kontrollkästchen **CognosPortlet**, aktivieren Sie es und klicken Sie auf **OK**, um das Portlet dem Seitenlayout hinzuzufügen. Eine Nachricht wird angezeigt, die bestätigt, dass das Portlet hinzugefügt wurde.
7. Wiederholen Sie Schritte 5 und 6, um zusätzliche Portlets hinzuzufügen. Sie können bis zu sechs Portlets hinzufügen.
8. Klicken Sie auf **Fertig**.

Nächste Schritte

Sie können die gemeinsamen Einstellungen für jedes Portlet bearbeiten. Klicken Sie im zu bearbeitenden Portlet oben rechts auf den Pfeil und wählen Sie im Menü die Option **Gemeinsame Einstellungen bearbeiten** aus. Weitere Informationen finden Sie unter „Portlet für die Anzeige von Berichten anpassen”.

Portlet für die Anzeige von Berichten anpassen

Verwenden Sie diese Informationen in diesem Thema, um ein IBM Intelligent Operations Center-Portlet für die Anzeige von IBM Cognos Business Intelligence-Berichten anzupassen.

Vorgehensweise

1. Melden Sie sich als Administrator beim Lösungsportal an.

2. Wählen Sie die Ansicht und das Portlet aus, die bzw. das zum Anzeigen von Berichten angepasst werden soll.
3. Navigieren Sie zum Anzeigemenü des Portlets in der rechten oberen Ecke des Portlets.
4. Klicken Sie auf **Edit Shared Settings** (Gemeinsam genutzte Einstellungen bearbeiten).
5. Geben Sie Ihre Einstellungen in den bereitgestellten Feldern ein.
   a. Geben Sie einen Titel für den Bericht ein.
   b. Geben Sie die **URL** für den Bericht ein. Suchen Sie die erforderliche URL wie im Thema „Berichts-URL lokalisieren" beschrieben.

      ```
      Beispiel: CAP_events_by_type_status_and_date:
      http://9.161.84.100:9082/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run
      &ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_model%27%5d%2ffolder%5b%40n
      ame%3d%27reports%27%5d%2freport%5b%40name%3d%27CAP_events_by_type_status_and_d
      ate%27%5d&ui.name=CAP_events_by_type_status_and_date&run.outputFormat=&run.prompt=tr
      ue
      ```

   c. Setzen Sie für das Portal den Wert für **Breite** auf *600*.
   d. Setzen Sie für das Portal den Wert für **Höhe** auf *600*.
   e. Klicken Sie auf **Speichern**.
   f. Klicken Sie im Portletanzeigemenü auf **Back** (Zurück), um zur Hauptportletansicht zurückzukehren.

Ergebnisse

Das Berichtsportlet wird aktualisiert und zeigt nun den zuletzt ausgewählten Bericht an.

Berichts-URL lokalisieren

In diesem Thema sind die Schritte zum Lokalisieren der URL für einen Bericht enthalten.

Vorgehensweise

1. Melden Sie sich bei IBM Cognos Connection an.
2. Navigieren Sie zu **Public Folders** > **ioc_model** > **reports** (Öffentliche Ordner > IOC-Modell > Berichte).
3. Wählen Sie einen Bericht aus und klicken Sie auf das Symbol **Set properties** (Eigenschaften festlegen).
4. Klicken Sie auf der Registerkarte **General** (Allgemein) auf **View the search path, ID and URL** (Suchpfad, ID und URL anzeigen), um die Berichts-URL anzuzeigen.
5. Kopieren Sie im Abschnitt **Default action URL** (Standardaktions-URL) die URL und fügen Sie sie nach Bedarf in das Portlet ein.

Mit dem Datenmodell arbeiten

IBM Intelligent Operations Center stellt zwei Datenmodelle bereit, die beim Generieren von Berichten verwendet werden. Ein Metamodell definiert die Sprache und die Prozesse, aus denen ein Modell gebildet wird.

Berichte in IBM Intelligent Operations Center werden auf der Basis von zwei Datenmodellen gebildet.

- Datenmodell des allgemeinen Schemas
- Datenmodell des CAP-Schemas (Common Alerting Protocol)

Beide IBM Intelligent Operations Center-Datenmodelle sind als Schichten organisiert. Für Berichtsersteller wird die Präsentationsansicht oder Schicht zur Verfügung gestellt. Sie besteht aus den folgenden Namespaces:

Business
: Enthält Wörterbücher, Filter und Daten.

Dimensional
Enthält Ereignisdimensionen für Berichte und Analysen.

Custom Query (Benutzerdefinierte Abfrage)
Enthält Abfragesubjekte, mit denen Sie benutzerdefinierte Abfragen für die relationale Berichtserstellung erstellen können.

Allgemeine Schemadatenmodellberichte generieren

In diesem Thema wird beschrieben, wie allgemeine Schemadatenmodellberichte generiert werden. Diese Berichte unterstützen Manager und Systemadministratoren bei der Überwachung aktueller Ereignisse, bei der Bearbeitung auftretender Ereignisse und bei der Planung zukünftiger Ereignisse.

Informationen zu diesem Vorgang

Führen Sie mithilfe der IBM Intelligent Operations Center-Konsole diese Schritte durch, um allgemeine Schemadatenmodellberichte zu generieren. Eine Beschreibung der Optionen zum Generieren eines Berichts erhalten Sie über die Referenzlinks am Ende des Themas.

Vorgehensweise

1. Klicken Sie in der IBM Intelligent Operations Center-Konsole in der Registerkarte "Administration" auf **Intelligent Operations** > **Administration Tools** > **Administration Consoles** (Intelligent Operations > Verwaltungstools > Administrationskonsolen). Die Seite für die Administrationskonsolen wird angezeigt.
2. Klicken Sie unter "Anwendungsserver" auf **Berichtsadministration**. Die IBM Cognos Connection-Seite wird angezeigt.
3. Klicken Sie auf **ioc common model** (Allgemeines IOC-Modell). Die öffentlichen Cognos-Ordner werden angezeigt.
4. Klicken Sie auf **Reports** (Berichte).
5. Wählen Sie den Typ des Berichts aus, den Sie generieren möchten:
   - Um einen Kreisdiagrammbericht zu generieren, klicken Sie auf **Pie charts** (Kreisdiagramme). Die allgemeinen Schemakreisdiagrammberichte werden angezeigt.
   - Um einen Tabellendiagrammbericht zu generieren, klicken Sie auf **Table charts** (Tabellendiagramme). Die allgemeinen Schematabellendiagrammberichte werden angezeigt.
6. Wählen Sie den Bericht aus, den Sie generieren möchten.

Optionen für Kreisdiagramme:

In diesem Thema werden die Optionen beschrieben, die Sie für allgemeine Kreisdiagrammberichte auswählen können.

Um auf diese Kreisdiagrammberichte über die IBM Cognos Connection-Seite zuzugreifen, klicken Sie auf **Public Folders** > **ioc_common_model** > **reports** > **Pie charts** (Öffentliche Ordner > Allgemeines IOC-Modell > Berichte > Kreisdiagramme).

Tabelle 65. Kreisdiagrammoptionen für allgemeine Schemadatenmodellberichte

Bericht	Beschreibung
Event by category (Ereignis nach Kategorie)	Zeigt Ereignisse nach Ereigniskategorie an. So können Sie beispielsweise alle Ereignisse in Zusammenhang mit Umwelt, Feuer oder Transport anzeigen.
Event by certainty (Ereignis nach Gewissheit)	Zeigt Ereignisse nach der Wahrscheinlichkeit an, mit der sie auftreten werden. Ist es beispielsweise zu einem Verkehrsunfall gekommen, ist die Gewissheit "Beobachtet".
Event by date sent (Ereignis nach Sendedatum)	In diesem Bericht werden Ereignisse angegeben, die an einem bestimmten Datum gesendet wurden.

Tabelle 65. Kreisdiagrammoptionen für allgemeine Schemadatenmodellberichte (Forts.)

Bericht	Beschreibung
Event by event type (Ereignis nach Ereignistyp)	Zeigt die Ereignisse nach Typ an. So kann es sich bei einem Ereignis beispielsweise um einen heraufziehenden Wirbelsturm oder einen Verkehrsunfall handeln.
Event by headline (Ereignis nach Überschrift)	Zeigt Ereignisse nach der Beschreibung an, die beim Erstellen eines Ereignisses eingegeben wurde. Daher entspricht die Überschrift hier der Ereignisbeschreibung.
Event by severity (Ereignis nach Schweregrad)	Zeigt Ereignisse nach Schweregrad an. Ereignisse können beispielsweise als "Extrem" oder "Schwerwiegend" eingestuft werden.
Event by specification (Ereignis nach Spezifikation)	Zeigt Ereignisse nach Spezifikation an. Ein Ereignis kann beispielsweise ein Common Alerting Protocol- oder ein kein Common Alerting Protocol-Ereignis sein. In diesem Diagramm wird daher der Prozentsatz von Common Alerting Protocol- und kein Common Alerting Protocol-Ereignissen angezeigt.
Event by urgency (Ereignis nach Dringlichkeit)	Zeigt Ereignisse nach ihrer Dringlichkeit an. So kann das Ereignis beispielsweise auftreten und mit dem Begriff "sofort" beschrieben werden.
Event by URL (Ereignis nach URL)	Zeigt Ereignisse nach der URL an, die beim Erstellen eines Ereignisses eingegeben wurde.

Optionen für das Tabellendiagramm:

In diesem Thema werden die Informationen beschrieben, die Sie für allgemeine Tabellendiagrammberichte generieren können.

Um auf diese Tabellendiagrammoptionen über die IBM Cognos Connection-Seite zuzugreifen, klicken Sie auf **Public Folders** > **ioc_common_model** > **reports** > **Table charts** (Öffentliche Ordner > Allgemeines IOC-Modell > Berichte > Tabellendiagramme).

Die einzige Tabellendiagrammoption für allgemeine Schemadatenmodellberichte ist die Ereignisliste. Die Ereignisliste ist eine vollständige Liste von Ereignissen mit detaillierten Informationen zu jedem Ereignis. Einige Beispiele dieser Informationen in der Ereignisliste werden nachstehend erläutert.

Tabelle 66. Informationen in der Ereignisliste für allgemeine Tabellendiagramme

Berichtsfeld	Beschreibung
ID	Identifiziert den Bericht.
Externe Ereignis-ID	Die Ereignis-ID, die beim Erstellen des Ereignisses generiert wird.
Spezifikation	Gibt an, ob das Ereignis ein Common Alerting Protocol- oder ein non-Common Alerting Protocol-Ereignis ist.
Ereignistyp	Zeigt die Ereignisse nach Typ an. So kann es sich bei einem Ereignis beispielsweise um einen heraufziehenden Wirbelsturm oder einen Verkehrsunfall handeln.
Gesendet	Datum und Uhrzeit, an dem bzw. zu der das Ereignis gesendet wurde.
Überschrift	Beschreibung des Ereignisses.
Kategorie	Zeigt Ereignisse nach Ereigniskategorie an. So können Sie beispielsweise alle Ereignisse in Zusammenhang mit Umwelt, Feuer oder Transport anzeigen.

Tabelle 66. Informationen in der Ereignisliste für allgemeine Tabellendiagramme (Forts.)

Berichtsfeld	Beschreibung
Gewissheit	Zeigt Ereignisse nach der Wahrscheinlichkeit an, mit der sie auftreten werden. Ist es beispielsweise zu einem Verkehrsunfall gekommen, ist die Gewissheit "Beobachtet".
Schweregrad	Zeigt Ereignisse nach Schweregrad an. Ereignisse können beispielsweise als "Extrem" oder "Schwerwiegend" eingestuft werden.
Dringlichkeit	Zeigt Ereignisse nach ihrer Dringlichkeit an. So kann das Ereignis beispielsweise auftreten und mit dem Begriff "sofort" beschrieben werden.
URL	Die URL zu diesem Bericht.

Common Alerting Protocol-Schemadatenmodellberichte generieren

In diesem Thema wird beschrieben, wie Common Alerting Protocol-Schemadatenmodellberichte generiert werden. Diese Berichte unterstützen Manager und Systemadministratoren bei der Überwachung aktueller Ereignisse, bei der Bearbeitung auftretender Ereignisse und bei der Planung zukünftiger Ereignisse.

Informationen zu diesem Vorgang

Führen Sie mithilfe der IBM Intelligent Operations Center-Konsole diese Schritte durch, um Common Alerting Protocol-Schemadatenmodellberichte zu generieren. Eine Beschreibung der Optionen zum Generieren eines Berichts erhalten Sie über die Referenzlinks am Ende des Themas.

Vorgehensweise

1. Klicken Sie in der IBM Intelligent Operations Center-Konsole in der Registerkarte "Administration" auf **Intelligent Operations** > **Administration Tools** > **Administration Consoles** (Intelligent Operations > Verwaltungstools > Administrationskonsolen). Die Seite für die Administrationskonsolen wird angezeigt.
2. Klicken Sie unter "Anwendungsserver" auf **Berichtsadministration**. Die IBM Cognos Connection-Seite wird angezeigt.
3. Klicken Sie auf **ioc cap model** (IOC-Cap-Modell). Die öffentlichen Cognos-Ordner werden angezeigt.
4. Klicken Sie auf **Reports** (Berichte).
5. Wählen Sie den Typ des Berichts aus, den Sie generieren möchten:
   - Um einen Datenmodellbericht zu generieren, der auf dieser Seite angezeigt wird, wählen Sie den Bericht aus.
   - Um einen Kreisdiagrammbericht zu generieren, klicken Sie auf **Pie charts** (Kreisdiagramme). Die allgemeinen Schemakreisdiagrammberichte werden angezeigt. Wählen Sie den Bericht aus der Liste aus.
   - Um einen benutzerdefinierten Bericht zu generieren, klicken Sie auf **User-defined reports** (Benutzerdefinierte Berichte). Die angepasste Cognos-Berichtsseite wird angezeigt. Füllen Sie die Felder für den angepassten Bericht aus und klicken Sie auf **Update** (Aktualisieren).

Datenmodell-Berichtsoptionen:

In diesem Thema werden die Optionen beschrieben, die Sie für den Common Alerting Protocol-Bericht auswählen können.

Um auf diese Berichtsoptionen über die IBM Cognos Connection-Seite zuzugreifen, klicken Sie auf **Public Folders** > **ioc_cap_model** > **reports** (Öffentliche Ordner > IOC-Cap-Modell > Berichte).

Tabelle 67. Optionen für Informationen zu den Common Alerting Protocol-Berichten

Bericht	Beschreibung
Common Alerting Protocol events by type, status, and date (Common Alerting Protocol-Ereignisse nach Typ, Status und Datum)	In diesem Bericht werden Common Alerting Protocol-Ereignisse nach Ereignistyp, Ereignisstatus und Ereignisdatum angezeigt. Beispiel: Der Ereignistyp könnte zufällig sein und der Status dringend. Das Datum könnte das heutige Datum sein.
Common Alerting Protocol events KPI metrics by date (Common Alerting Protocol-Ereignis-KPI-Metriken nach Datum)	In diesem Bericht werden Common Alerting Protocol-Ereignisse auf der Grundlage der KPI-Metriken für ein bestimmtes Datum oder für einen Datumsbereich angezeigt.
Common Alerting Protocol events KPI metrics by department (Common Alerting Protocol-Ereignis-KPI-Metriken nach Abteilung)	In diesem Bericht werden Common Alerting Protocol-Ereignisse nach KPI-Metrik für eine bestimmte Abteilung oder für einen bestimmten Bereich angezeigt. Beispiel: Im Bericht könnten KPI-Metriken für die Wasserabteilung oder für einen bestimmten Stadtbezirk angezeigt werden.
Common Alerting Protocol full details (Vollständige Common Alerting Protocol-Details)	In diesem Bereich werden Details zu Common Alerting Protocol-Ereignissen angezeigt. Beispiel: Details zur Common Alerting Protocol-ID, zum Sender, zum Sendedatum und zur Sendezeit, zum Status, zum Nachrichtentyp, zur Quelle und zu weiteren Faktoren.
IBM Intelligent Operations Center events by severity anytime (IBM® Intelligent Operations Center-Ereignisse nach Schweregrad zu jeder Zeit)	In diesem Bericht werden alle IBM Intelligent Operations Center-Ereignisse nach Schweregrad angezeigt. Beispiel: Ereignisse könnten als "Extrem" eingestuft werden.
IBM Intelligent Operations Center events by severity in progress (IBM Intelligent Operations Center-Ereignisse nach Schweregrad in Bearbeitung)	In diesem Bericht werden alle IBM Intelligent Operations Center-Ereignisse nach Schweregrad aufgelistet, die zurzeit auftreten. Beispiel: Der Schweregrad in Bearbeitung könnte ein extremes Wetter sein, das zurzeit herrscht.

Optionen für Kreisdiagramme:

In diesem Thema werden die Optionen beschrieben, die Sie zum Generieren von Common Alerting Protocol-Kreisdiagrammberichten haben.

Um auf diese Kreisdiagrammoptionen über die IBM Cognos Connection-Seite zuzugreifen, klicken Sie auf **Public Folders** > **ioc_cap_model** > **reports** > **Pie charts** (Öffentliche Ordner > IOC-Cap-Modell > Berichte > Kreisdiagramme).

Tabelle 68. Optionen für Informationen zu den Common Alerting Protocol-Kreisdiagrammberichten

Bericht	Beschreibung
Cap by category (CAP nach Kategorie)	Zeigt Common Alerting Protocol nach einer bestimmten Kategorie an. So können Sie beispielsweise alle Ereignisse in Zusammenhang mit Umwelt, Feuer oder Transport anzeigen.
Cap by certainty (CAP nach Gewissheit)	Zeigt Common Alerting Protocol-Ereignisse nach der Wahrscheinlichkeit ihres Auftretens an. Ist es beispielsweise zu einem Verkehrsunfall gekommen, ist die Gewissheit "Beobachtet".
Cap by date sent (CAP nach Sendedatum)	Zeigt Common Alerting Protocol-Ereignisse an, die an einem bestimmten Datum gesendet wurden.
Cap by event type (CAP nach Ereignistyp)	Zeigt Common Alerting Protocol-Ereignisse nach Typ an. So kann es sich bei einem Ereignis beispielsweise um einen heraufziehenden Wirbelsturm oder einen Verkehrsunfall handeln.

Tabelle 68. Optionen für Informationen zu den Common Alerting Protocol-Kreisdiagrammberichten (Forts.)

Bericht	Beschreibung
Cap by handling code (CAP nach Bearbeitungscode)	Zeigt Common Alerting Protocol-Ereignisse nach Bearbeitungscode an. Beispiel für einen Bearbeitungscode ist "Ereignis".
Cap by message type (CAP nach Nachrichtentyp)	Zeigt Common Alerting Protocol-Ereignisse nach Nachrichtentyp (z. B. Aktualisierungen oder Alerts) an.
Cap by scope (CAP nach Geltungsbereich)	Zeigt Common Alerting Protocol-Ereignisse nach Umfang an. Der Geltungsbereich eines Ereignis kann beispielsweise "öffentlich" sein.
Cap by sender (CAP nach Sender)	Zeigt Common Alerting Protocol-Ereignisse nach dem Namen des Senders an.
Cap by severity (CAP nach Schweregrad)	Zeigt Common Alerting Protocol-Ereignisse nach Schweregrad an. Ereignisse können beispielsweise als "Extrem" oder "Schwerwiegend" eingestuft werden.
Cap by source (CAP nach Quelle)	Zeigt Common Alerting Protocol nach einer bestimmten Quelle an. Die Quelle kann z. B. "Transport" sein.
Cap by status (CAP nach Status)	Zeigt Common Alerting Protocol-Ereignisse nach Status an. Für den Status kann Folgendes angegeben werden: • Akzeptabel • Vorsicht • Take action (Maßnahme ergreifen)
Cap by urgency (CAP nach Dringlichkeit)	Zeigt Common Alerting Protocol-Ereignisse nach ihrer Dringlichkeit an. So kann das Ereignis beispielsweise auftreten und mit dem Begriff "sofort" beschrieben werden.
Notification by category (Benachrichtigung nach Kategorie)	Zeigt Alertnachrichten im Common Alerting Protocol-Format nach einer bestimmten Kategorie an. So können Sie beispielsweise alle Ereignisse in Zusammenhang mit Umwelt, Feuer oder Transport anzeigen.
Notification by type (Benachrichtigung nach Typ)	Zeigt Benachrichtigungen im Common Alerting Protocol-Format nach Typ an. Der Typ kann beispielsweise eine Aktualisierungen oder ein Alerts sein.

Benutzerdefinierte Optionen für Ereignisberichte:

In diesem Thema werden die Optionen beschrieben, die Ihnen zum Generieren von benutzerdefinierten-Common Alerting Protocol-Berichten für Ereignisse zur Verfügung stehen.

Um auf die benutzerdefinierten Berichte über die IBM Cognos Connection-Seite zuzugreifen, klicken Sie auf **Public Folders** > **ioc_cap_model** > **reports** > **User-defined_reports** > **Events** (Öffentliche Ordner > IOC-Cap-Modell > Berichte > Benutzerdefinierte Berichte > Ereignisse).

Tabelle 69. Common Alerting Protocol-Ereignisoptionen

Bericht	Beschreibung
Events by Category Anytime (Ereignisse nach Kategorie zu jeder Zeit)	Zeigt unabhängig vom Datum alle Ereignisse nach Kategorie an. So können Sie beispielsweise alle Ereignisse in Zusammenhang mit Umwelt, Feuer oder Transport anzeigen.
Events by Certainty Anytime (Ereignisse nach Gewissheit zu jeder Zeit)	Zeigt unabhängig vom Datum alle Ereignisse nach Gewissheit an. Ist es beispielsweise zu einem Verkehrsunfall gekommen, ist die Gewissheit "Beobachtet".

Tabelle 69. Common Alerting Protocol-Ereignisoptionen (Forts.)

Bericht	Beschreibung
Events by Event Anytime (Ereignisse nach Ereignis zu jeder Zeit)	Zeigt unabhängig vom Datum alle Ereignisse nach Ereignis an. So kann es sich bei Ereignissen beispielsweise um heraufziehende Wirbelstürme oder Verkehrsunfälle handeln, die an einem beliebigen Datum aufgetreten sind.
Events by Severity Anytime (Ereignisse nach Schweregrad zu jeder Zeit)	Zeigt unabhängig vom Datum alle Ereignisse nach Schweregrad an. Es werden beispielsweise extreme oder schwerwiegende Ereignisse angezeigt, die an einem beliebigen Datum aufgetreten sind.
Events by Urgency Anytime (Ereignisse nach Dringlichkeit zu jeder Zeit)	Zeigt unabhängig vom Datum alle Ereignisse nach Dringlichkeit an. So können Ereignisse beispielsweise auftreten und mit dem Begriff "sofort" beschrieben werden.

Benutzerdefinierte, angepasste Berichtsoptionen:

In diesem Thema werden die Optionen beschrieben, die Ihnen zum Generieren von benutzerdefinierten, angepassten Common Alerting Protocol-Berichten zur Verfügung stehen.

Mithilfe des Berichtsportlets können Sie für Ereignisse einen benutzerdefinierten Bericht erstellen. Wählen Sie dazu zunächst aus, wie die Ereignisse gruppiert werden sollen. Sollen beispielsweise alle Ereignisse angezeigt werden, die zu einer bestimmten Kategorie gehören, wählen Sie in dem Feld, in dem die Anordnung der Ereignisse angegeben werden kann, die Option **Kategorie** aus. Dann können Sie in den Feldern für die Auswahl der Daten die Daten in Zusammenhang mit den Informationen eingeben, die angezeigt werden sollen. Darüber hinaus können Sie für die Ereignisse im Bericht ein bestimmtes Datum oder einen bestimmten Zeitraum angeben. Wenn Sie anschließend auf **Aktualisieren** klicken, werden im Diagramm die gewünschten Informationen angezeigt.

Um die URL für den neuen Bericht abzurufen, klicken Sie auf die Option zum Abruf der Berichts-URL.

Um auf die angepasste, benutzerdefinierte IBM Cognos Connection-Seite zuzugreifen, klicken Sie auf **Public Folders** > **ioc_cap_model** > **reports** > **User-defined_reports** > **User-defined report** (Öffentliche Ordner > IOC-Cap-Modell > Berichte > Benutzerdefinierte Berichte > Benutzerdefinierter Bericht).

Tabelle 70. Benutzerdefinierte, angepasste Common Alerting Protocol-Optionen

Bericht	Beschreibung
Anordnen nach	Wählen Sie die Option aus, nach der Ereignisse gruppiert werden sollen.
Schweregrad	Zeigt Ereignisse nach Schweregrad an. Ereignisse können beispielsweise als "Extrem" oder "Schwerwiegend" eingestuft werden.
Gewissheit	Zeigt Ereignisse nach der Wahrscheinlichkeit an, mit der sie auftreten werden. Ist es beispielsweise zu einem Verkehrsunfall gekommen, ist die Gewissheit "Beobachtet".
Dringlichkeit	Zeigt Ereignisse nach ihrer Dringlichkeit an. So kann das Ereignis beispielsweise auftreten und mit dem Begriff "sofort" beschrieben werden.
Ereigniskategorie	Zeigt Ereignisse nach Ereigniskategorie an. So können Sie beispielsweise alle Ereignisse in Zusammenhang mit Umwelt, Feuer oder Transport anzeigen.

Tabelle 70. Benutzerdefinierte, angepasste Common Alerting Protocol-Optionen (Forts.)

Bericht	Beschreibung
Ereignistyp	Zeigt die Ereignisse nach Typ an. So kann es sich bei einem Ereignis beispielsweise um einen heraufziehenden Wirbelsturm oder einen Verkehrsunfall handeln.
Anfangsdatum	Geben Sie das Datum an, für das Ereignisse angezeigt werden sollen. Bei Angabe eines Zeitraums wird hier das Anfangsdatum eingegeben.
Enddatum	Geben Sie hier das Datum ein, bis zu dem Ereignisse angezeigt werden sollen.

Allgemeine Schemadatenmodellberichte konfigurieren

In diesem Thema wird beschrieben, wie Sie allgemeine und spezifische Eigenschaften für allgemeine Schemadatenmodellberichte festlegen.

Vorbereitende Schritte

Sie benötigen einen Administratorzugriff, um dies durchzuführen.

Informationen zu diesem Vorgang

Verwenden Sie die IBM Intelligent Operations Center-Konsole, um diese Berichte zu konfigurieren.

Vorgehensweise

1. Klicken Sie in der IBM Intelligent Operations Center-Konsole in der Registerkarte "Administration" auf **Intelligent Operations** > **Administration Tools** > **Administration Consoles** (Intelligent Operations > Verwaltungstools > Administrationskonsolen). Die Seite für die Administrationskonsolen wird angezeigt.
2. Klicken Sie unter "Anwendungsserver" auf **Berichtsadministration**. Die IBM Cognos Connection-Seite wird angezeigt.
3. Aktivieren Sie das Kontrollkästchen **ioc common model** (Allgemeines IOC-Modell) und klicken Sie dann auf **More** (Weitere). Die Seite "Available Actions" (Verfügbare Aktionen) wird angezeigt.
4. Klicken Sie auf **Set properties** (Eigenschaften festlegen). Die Seite "General properties" (Allgemeine Eigenschaften) wird angezeigt.
5. Wählen Sie die Werte für die allgemeinen Berichtseigenschaften aus.
6. Wählen Sie in der Registerkarte "Permissions" (Berechtigungen) die Berechtigungen für die allgemeinen Schemadatenmodellberichte aus.
7. Wählen Sie in der Registerkarte "Capabilities" (Funktionen) die Funktionen für die Berichte aus.
8. Klicken Sie auf **OK**.

Common Alerting Protocol-Schemadatenmodellberichte konfigurieren

In diesem Thema wird beschrieben, wie Sie allgemeine Eigenschaften und Berechtigungen festlegen und Benutzertypen für Common Alerting Protocol-Schemadatenmodellberichte Funktionen zuweisen können.

Vorbereitende Schritte

Sie benötigen einen Administratorzugriff, um dies durchzuführen.

Informationen zu diesem Vorgang

Verwenden Sie die IBM Intelligent Operations Center-Konsole, um diese Berichte zu konfigurieren.

Vorgehensweise

1. Klicken Sie in der IBM Intelligent Operations Center-Konsole in der Registerkarte "Administration" auf **Intelligent Operations** > **Administration Tools** > **Administration Consoles** (Intelligent Operations > Verwaltungstools > Administrationskonsolen). Die Seite für die Administrationskonsolen wird angezeigt.
2. Klicken Sie unter "Anwendungsserver" auf **Berichtsadministration**. Die IBM Cognos Connection-Seite wird angezeigt.
3. Aktivieren Sie das Kontrollkästchen **ioc cap model** (IOC-Cap-Modell) und klicken Sie dann auf **More** (Weitere). Die Seite "Available Actions" (Verfügbare Aktionen) wird angezeigt.
4. Klicken Sie auf **Set properties** (Eigenschaften festlegen). Die Seite "General properties" (Allgemeine Eigenschaften) wird angezeigt.
5. Wählen Sie die Werte für die allgemeinen Berichtseigenschaften aus.
6. Wählen Sie in der Registerkarte "Permissions" (Berechtigungen) die Berechtigungen für die Common Alerting Protocol-Schemadatenmodellberichte aus.
7. Wählen Sie in der Registerkarte "Capabilities" (Funktionen) die Funktionen für die Benutzer des Berichts aus.
8. Klicken Sie auf **OK**.

Weitere Berichtsoptionen

In diesem Thema werden zusätzliche Berichtsoptionen für allgemeine und Common Alerting Protocol-Berichte beschrieben.

Klicken Sie zum Zugreifen auf diese Optionen rechts neben dem Link für einen bestimmten Bericht auf **More** (Weitere).

Tabelle 71. Für jeden Bericht zusätzlich verfügbare Optionen

Option	Beschreibung
Set properties (Eigenschaften festlegen)	Legen Sie allgemeine Eigenschaften für den ausgewählten Bericht fest.
View report output version (Berichtsausgabeversion anzeigen)	Wählen Sie die anzuzeigende Ausgabeversion aus, indem Sie auf einen Format-Hyperlink klicken.
View my permissions (Berechtigungen anzeigen)	Zeigen Sie die Zugriffsberechtigungen für diesen Eintrag an.
Run with options (Mit Optionen ausführen)	Wählen Sie aus, wie Sie Ihren Bericht ausführen und erhalten möchten. Beispiele sind unter anderem HTML und PDF.
Open with Report Studio (Mit Report Studio öffnen)	Zeigen Sie den Bericht mithilfe von Report Studio in einem anderen Browser an.
Open with Business Insight Advanced (Mit Business Insight Advanced öffnen)	Zeigen Sie den Bericht mithilfe von IBM Cognos Business Insight Advanced in einem anderen Browser an.
New schedule (Neuer Plan)	Planen Sie einen Bericht mithilfe verschiedener Kriterien.
Move (Verschieben)	Verschieben Sie einen Bericht an eine andere Position.
Copy (Kopieren)	Kopieren Sie einen Bericht an eine andere Position.
Create a shortcut to this entry (Verknüpfung zum Eintrag erstellen)	Erstellen Sie eine Verknüpfung auf Ihrem Desktop, um auf den Bericht zugreifen zu können.
Create a report view of this report (Berichtsanzeige des Berichts erstellen)	Erstellen Sie eine Anzeige auf Ihrem Desktop für den Bericht, der in einem lokalen Verzeichnis gespeichert ist.
Delete (Löschen)	Löschen Sie den angezeigten Bericht.

Kapitel 6. Verwaltung der Lösung

Die Themen in diesem Abschnitt beschreiben die Vorgehensweise zur Ausführung von administrativen Aufgaben für IBM Intelligent Operations Center.

Produktinformationen

Im Portlet "Produktinformationen" können Sie Details zur Version des IBM Intelligent Operations Center und zur Version der integrierten IBM Smarter Cities Software Solutions anzeigen, die Sie installiert haben. Außerdem können Sie Details zu allen Aktualisierungen anzeigen, die Sie seit der Installation ausgeführt haben.

Starten Sie das Portlet "Produktinformationen", indem Sie in der WebSphere Portal-Verwaltungsschnittstelle auf "**Intelligent Operations** > **About** (Intelligent Operations > About)" klicken.

Das Portlet "Produktinformationen" stellt die folgenden Informationen zur Verfügung:

- Die Position von allen installierten Softwareprodukten und -komponenten
- Den Namen und die Version der installierten Produkte
- Den Namen und die Version der installierten Komponenten
- Die Details zu allen ausgeführten Fixes

Bei den angegebenen Komponenten handelt es sich um Komponenten oder Bereiche eines Produkts. Beispiele:

- Ein Produktbereich, für den eine bestimmte Wartung oder ein gezielter Servicedatenstrom vorgesehen wurde
- Ein optional installierbarer Produktbereich
- Produktbereiche, die von mehreren Produkten gemeinsam genutzt werden

Anmerkung: Die für die einzelnen Fixes angezeigten Informationen hängen von der Ausführung des entsprechenden Schritts ab, der in den Installationsanweisungen zu dem betreffenden Fix genannt wird.

Portlet "Produktinformationen" anpassen

Sie haben die Möglichkeit, dieses Portlet anzupassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Zugehörige Tasks:

„Installation überprüfen” auf Seite 55
Überprüfen Sie nach der Installation von IBM Intelligent Operations Center dass das Produkt ordnungsgemäß installiert wurde.

Zugehörige Verweise:

„Einstellungen des Produktinformationen-Portlets” auf Seite 154
Anpassen des Produktinformationen-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Services steuern

Die auf den IBM Intelligent Operations Center-Servern ausgeführten IBM Intelligent Operations Center Services können gesteuert und abgefragt werden.

Services starten

Zum Starten von Services, die auf IBM Intelligent Operations Center-Servern ausgeführt werden, ist das Plattformsteuerungstool verfügbar.

Informationen zu diesem Vorgang

Der Befehl **IOCControl.sh** muss als Benutzer ibmadmin ausgeführt werden. Sind Sie nicht als ibmadmin angemeldet, wechseln Sie mit dem Befehl **su - ibmadmin** zum Benutzeraccount ibmadmin.

Achtung: Das Starten einzelner Services sollte nur von erfahrenen IBM Intelligent Operations Center-Administratoren durchgeführt werden. Es kann zu unvorhersehbaren Ergebnissen kommen, wenn die Services nicht in der erforderlichen Reihenfolge gestartet werden.

Vorgehensweise

Führen Sie auf dem Verwaltungsserver den folgenden Befehl aus, um alle IBM Intelligent Operations Center-Services zu starten.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start all Kennwort
```

Hierbei ist *Kennwort* das Kennwort für das Plattformsteuerungstool, das bei der Installation von Plattformsteuerungstool definiert wurde.
Die Services werden in der erforderlichen Reihenfolge gestartet. Grundsätzlich erforderliche Services werden vor abhängigen Services gestartet. Datenbank- und Verzeichnisservices werden z. B. als Erstes gestartet.
Führen Sie den folgenden Befehl aus, um nur einen Service zu starten.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start Service-ID Kennwort
```

Hierbei ist *Service-ID* eine Kennung, die unter **Zieloptionen** im Hilfetext von **IOCControl** aufgelistet ist und *Kennwort* das Kennwort für das Plattformsteuerungstool, das bei der Installation von Plattformsteuerungstool definiert wurde.

Ergebnisse

Die erforderlichen IBM Intelligent Operations Center-Services wurden gestartet.

Nächste Schritte

Überprüfen Sie nach der Ausführung des Befehls **IOCControl.sh** die Protokolle im Verzeichnis /opt/IBM/ISP/mgmt/logs. Diese Protokolle enthalten das Ergebnis der Ausführung von **IOCControl.sh**.

Zugehörige Tasks:

„Services stoppen" auf Seite 209
Zum Stoppen von IBM Intelligent Operations Center-Services ist das Plattformsteuerungstool verfügbar.

„Status der Services abfragen" auf Seite 212
Das Plattformsteuerungstool ist für die Bestimmung des Status von IBM Intelligent Operations Center-Services verfügbar.

„Hilfe für das Plattformsteuerungstool abrufen" auf Seite 213
Es sind Informationen zu Aktions- und Zieloptionen für das Plattformsteuerungstool verfügbar.

„Installation überprüfen" auf Seite 55
Überprüfen Sie nach der Installation von IBM Intelligent Operations Center dass das Produkt ordnungsgemäß installiert wurde.

„Plattformsteuerungstool installieren" auf Seite 53
Das Plattformsteuerungstool wird verwendet, um die Serverumgebung von IBM Intelligent Operations Center zu verwalten. Das Tool wird getrennt vom Produkt installiert.

„Das Tool Systemprüfung installieren" auf Seite 54
Das Tool Systemprüfung wird verwendet, um den Betriebsstatus von Komponenten in IBM Intelligent Operations Center zu überprüfen. Das Tool wird getrennt vom Produkt installiert.

Erforderliche Startreihenfolge

IBM Intelligent Operations Center-Services müssen in einer bestimmten Reihenfolge gestartet werden.

Zum Starten von IBM Intelligent Operations Center-Services wird das Plattformsteuerungstool verwendet. Es wird empfohlen, alle Services mit der Option **`start all`** des Plattformsteuerungstool zu starten. Allerdings kann es Fälle geben, in denen Services einzeln gestartet werden müssen.

Manche Services stehen in Abhängigkeit zu anderen Services, weshalb Services in einer bestimmten Reihenfolge gestartet werden müssen.

In der Regel sollten Services in drei Gruppen gestartet werden:

Gruppe 1
`tds`, `db24po`, `db24sms`, `db24wbm`, `db24ana`, `db24tsrm`, `db24sol`, `db24mgmt`

Gruppe 2
`ihs`, `appdmgr`, `st`

Gruppe 3
alle verbleibenden Services

Starten Sie die Services der Gruppe 1 zuerst, starten Sie dann Gruppe 2 und schließlich Gruppe 3. Die Services innerhalb jeder Gruppe können in beliebiger Reihenfolge gestartet werden.

Tabelle 72. Abhängigkeiten der Startreihenfolge der IBM Intelligent Operations Center-Services

Service	Beschreibung	Services, die aktiv sein müssen, bevor dieser Service gestartet wird
`db24po`	DB2 Enterprise Server Edition für WebSphere Portal Server	Keine
`db24wbm`	DB2 Enterprise Server Edition für WebSphere Business Modeler	Keine
`db24sol`	DB2 Enterprise Server Edition für IBM Intelligent Operations Center	Keine
`db24ana`	DB2 Enterprise Server Edition für Cognos	Keine
`db24mgmt`	DB2 Enterprise Server Edition für Tivoli Enterprise Portal-Services	Keine

Tabelle 72. Abhängigkeiten der Startreihenfolge der IBM Intelligent Operations Center-Services (Forts.)

Service	Beschreibung	Services, die aktiv sein müssen, bevor dieser Service gestartet wird
db24tsrm	DB2 Enterprise Server für Tivoli Service Request Manager	Keine
db24sms	DB2 Enterprise Server für Semantic Model Services	Keine
tds	Tivoli Directory Server	Keine
tdspxyapp	Tivoli Directory Server Proxy (Anwendungsserver)	tds
tdspxyevt	Tivoli Directory Server Proxy (Ereignisserver)	tds
tdspxymgt	Tivoli Directory Server Proxy (Verwaltungsserver)	tds
tdsappsrv	Tivoli Directory Server Anwendungsserver	Keine
tamps	Tivoli Access Manager Richtlinienserver	tamas
tamas	Tivoli Access Manager Berechtigungsserver	tds
tamwpm	Tivoli Access Manager Web Portal Manager	Keine
tamweb	Tivoli Access Manager WebSEAL	tamas
tems	Tivoli Monitoring Enterprise Monitoring Server	Keine
teps	Tivoli Monitoring Enterprise Portal Server	tems, db24mgmt
tim	Tivoli Identity Manager	tds
appdmgr	WebSphere Application Server Network Deployment	Keine
cplex	WebSphere Application Server für CPLEX	db24sms
ihs	HTTP Server für Runtime (Anwendungsserver)	Keine
ihsevt	HTTP Server für Runtime (Ereignisserver)	ihs
ihsmgt	HTTP Server für Runtime (Verwaltungsserver)	ihs
ncob	Tivoli Netcool/OMNIbus	Keine
nci	Tivoli Netcool/Impact	ncob
wbm	IBM WebSphere Business Monitor	db24wbm
st	Lotus Sametime	Keine
stpxy	Lotus Sametime-Proxy-Anwendungsserver	st
wpe	WebSphere Portal Extend	tdspxyapp, db24po, appdmgr
wmb	WebSphere Message Broker	Keine
cognos	IBM Cognos Business Intelligence	db24ana, appdmgr
tsrm	Tivoli Service Request Manager	appdmgr, db24tsrm
wodm	WebSphere Operations Decision Manager	appdmgr
wodmdc	WebSphere Operations Decision Manager (Decision Center)	Keine
smsclt	Semantic Model Services (Client-Services)	appdmgr
smsdaaq	Semantic Model Services (Datenservices)	appdmgr
smsmdl	Semantic Model Services (Modellservices)	appdmgr
smsmgmt	Semantic Model Services (Management-Services)	appdmgr
smsrtc	Semantic Model Services (RTC-Services)	appdmgr
iocxml	IBM Intelligent Operations Center XML-Testmonitor	db24sol

Tivoli Netcool/OMNIbus-Testmonitor starten und stoppen

Starten Sie den Tivoli Netcool/OMNIbus-Testmonitor, nachdem alle IBM Intelligent Operations Center-Server gestartet sind.

Informationen zu diesem Vorgang

Der Testmonitor ist Teil des IOCControl-Scripts. Der Testmonitor wird gestartet und gestoppt, wenn Sie Tivoli Netcool/OMNIbus starten und stoppen. Der Tivoli Netcool/OMNIbus-Testmonitor ist mit Tivoli Netcool/OMNIbus im Script verknüpft. Mit der folgenden Vorgehensweise können Sie den Testmonitor stoppen, starten sowie seinen Status überprüfen.

Vorgehensweise

1. Führen Sie zum Stoppen des Testmonitors auf dem Verwaltungsserver folgenden Befehl aus:
   ```
   /opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop ncob password
   ```
2. Führen Sie zum Starten des Testmonitors auf dem Verwaltungsserver folgenden Befehl aus:
   ```
   /opt/IBM/ISP/mgmt/scripts/IOCControl.sh start ncob password
   ```
3. So überprüfen Sie den Status des Testmonitors:
   - Führen Sie auf dem Verwaltungsserver den folgenden Befehl aus:
     ```
     /opt/IBM/ISP/mgmt/scripts/IOCControl.sh start iocxml password
     ```
   - Führen Sie auf dem Ereignisserver den folgenden Befehl aus:
     ```
     tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
     ```

Services stoppen

Zum Stoppen von IBM Intelligent Operations Center-Services ist das Plattformsteuerungstool verfügbar.

Informationen zu diesem Vorgang

Der Befehl **IOCControl.sh** muss als Benutzer ibmadmin ausgeführt werden. Sind Sie nicht als ibmadmin angemeldet, wechseln Sie mit dem Befehl **su - ibmadmin** zum Benutzeraccount ibmadmin.

Achtung: Das Stoppen einzelner Services sollte nur von erfahrenen IBM Intelligent Operations Center-Administratoren durchgeführt werden. Es kann zu unvorhersehbaren Ergebnissen kommen, wenn die Services nicht in der erforderlichen Reihenfolge gestoppt werden.

Vorgehensweise

Führen Sie auf dem Verwaltungsserver den folgenden Befehl aus, um alle IBM Intelligent Operations Center-Services zu stoppen.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop all Kennwort
```

Hierbei ist *Kennwort* das Kennwort für das Plattformsteuerungstool, das bei der Installation von Plattformsteuerungstool definiert wurde.
Führen Sie den folgenden Befehl aus, um nur einen Service zu stoppen.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop Service-ID Kennwort
```

Hierbei ist *Service-ID* eine Kennung, die unter **Zieloptionen** im Hilfetext von **IOCControl** aufgelistet ist und *Kennwort* das Kennwort für das Plattformsteuerungstool, das bei der Installation von Plattformsteuerungstool definiert wurde.

Ergebnisse

Die erforderlichen IBM Intelligent Operations Center-Services werden gestoppt.

Nächste Schritte

Überprüfen Sie nach der Ausführung des Befehls **IOCControl.sh** die Protokolle im Verzeichnis /opt/IBM/ISP/mgmt/logs. Diese Protokolle enthalten das Ergebnis der Ausführung von **IOCControl.sh**.

Zugehörige Tasks:

„Services starten" auf Seite 206
Zum Starten von Services, die auf IBM Intelligent Operations Center-Servern ausgeführt werden, ist das Plattformsteuerungstool verfügbar.

„Status der Services abfragen" auf Seite 212
Das Plattformsteuerungstool ist für die Bestimmung des Status von IBM Intelligent Operations Center-Services verfügbar.

„Hilfe für das Plattformsteuerungstool abrufen" auf Seite 213
Es sind Informationen zu Aktions- und Zieloptionen für das Plattformsteuerungstool verfügbar.

„Installation überprüfen" auf Seite 55
Überprüfen Sie nach der Installation von IBM Intelligent Operations Center dass das Produkt ordnungsgemäß installiert wurde.

„Plattformsteuerungstool installieren" auf Seite 53
Das Plattformsteuerungstool wird verwendet, um die Serverumgebung von IBM Intelligent Operations Center zu verwalten. Das Tool wird getrennt vom Produkt installiert.

„Das Tool Systemprüfung installieren" auf Seite 54
Das Tool Systemprüfung wird verwendet, um den Betriebsstatus von Komponenten in IBM Intelligent Operations Center zu überprüfen. Das Tool wird getrennt vom Produkt installiert.

Erforderliche Stoppreihenfolge

IBM Intelligent Operations Center-Services müssen in einer bestimmten Reihenfolge gestoppt werden.

Zum Stoppen von IBM Intelligent Operations Center-Services wird das Plattformsteuerungstool verwendet. Es wird empfohlen, alle Services mit der Option **stop all** des Plattformsteuerungstool zu stoppen. Allerdings kann es Fälle geben, in denen Services einzeln gestoppt werden müssen.

Manche Services stehen in Abhängigkeit zu anderen Services, weshalb Services in einer bestimmten Reihenfolge gestoppt werden müssen.

In der Regel sollten Services in drei Gruppen gestoppt werden:

Gruppe 1
`tds, db24po, db24sms, db24wbm, db24ana, db24tsrm, db24sol, db24mgmt`

Gruppe 2
`ihs, appdmgr, st`

Gruppe 3
alle verbleibenden Services

Stoppen Sie die Services der Gruppe 3 zuerst, stoppen Sie dann Gruppe 2 und schließlich Gruppe 1. Die Services innerhalb jeder Gruppe können in beliebiger Reihenfolge gestoppt werden.

Tabelle 73. Abhängigkeiten der Stoppreihenfolge der IBM Intelligent Operations Center-Services

Service	Beschreibung	Services, die bereits gestoppt sein müssen, bevor dieser Service gestoppt wird
db24po	DB2 Enterprise Server Edition für WebSphere Portal Server	wpe
db24wbm	DB2 Enterprise Server Edition für WebSphere Business Modeler	wbm

Tabelle 73. Abhängigkeiten der Stoppreihenfolge der IBM Intelligent Operations Center-Services (Forts.)

Service	Beschreibung	Services, die bereits gestoppt sein müssen, bevor dieser Service gestoppt wird
db24sol	DB2 Enterprise Server Edition für IBM Intelligent Operations Center	iocxml
db24ana	DB2 Enterprise Server Edition für Cognos	cognos
db24mgmt	DB2 Enterprise Server Edition für Tivoli Enterprise Portal-Services	teps
db24tsrm	DB2 Enterprise Server für Tivoli Service Request Manager	tsrm
db24sms	DB2 Enterprise Server für Semantic Model Services	cplex
tds	Tivoli Directory Server	tdsprxyapp, tdspxyevt, tdspxymgt, tamas, tim
tdspxyapp	Tivoli Directory Server Proxy (Anwendungsserver)	wpe
tdspxyevt	Tivoli Directory Server Proxy (Ereignisserver)	Keine
tdspxymgt	Tivoli Directory Server Proxy (Verwaltungsserver)	Keine
tdsappsrv	Tivoli Directory Server Anwendungsserver	Keine
tamps	Tivoli Access Manager Richtlinienserver	Keine
tamas	Tivoli Access Manager Berechtigungsserver	tamps
tamwpm	Tivoli Access Manager Web Portal Manager	Keine
tamweb	Tivoli Access Manager WebSEAL	Keine
tems	Tivoli Monitoring Enterprise Monitoring Server	teps
teps	Tivoli Monitoring Enterprise Portal Server	Keine
tim	Tivoli Identity Manager	Keine
appdmgr	WebSphere Application Server Network Deployment	wpe, cognos, tsrm, wodm, smsclt, smsdaaq, smsmdl, smsrtc, smsmgmt
cplex	WebSphere Application Server für CPLEX	Keine
ihs	HTTP Server für Runtime (Anwendungsserver)	ihsevt, ihsmgt
ihsevt	HTTP Server für Runtime (Ereignisserver)	Keine
ihsmgt	HTTP Server für Runtime (Verwaltungsserver)	Keine
ncob	Tivoli Netcool/OMNIbus	nci
nci	Tivoli Netcool/Impact	Keine
wbm	IBM WebSphere Business Monitor	Keine
st	Lotus Sametime	stpxy
stpxy	Lotus Sametime Proxy Application Server	Keine
wpe	WebSphere Portal Extend	Keine
wmb	WebSphere Message Broker	Keine
cognos	IBM Cognos Business Intelligence	Keine
tsrm	Tivoli Service Request Manager	Keine
wodm	WebSphere Operations Decision Manager	Keine
wodmdc	WebSphere Operations Decision Manager (Decision Center)	Keine
smsclt	Semantic Model Services (Client-Services)	Keine

Tabelle 73. Abhängigkeiten der Stoppreihenfolge der IBM Intelligent Operations Center-Services (Forts.)

Service	Beschreibung	Services, die bereits gestoppt sein müssen, bevor dieser Service gestoppt wird
smsdaaq	Semantic Model Services (Datenservices)	Keine
smsmdl	Semantic Model Services (Modellservices)	Keine
smsmgmt	Semantic Model Services (Management-Services)	Keine
smsrtc	Semantic Model Services (RTC-Services)	Keine
iocxml	IBM Intelligent Operations Center XML-Testmonitor	Keine

Status der Services abfragen

Das Plattformsteuerungstool ist für die Bestimmung des Status von IBM Intelligent Operations Center-Services verfügbar.

Informationen zu diesem Vorgang

Der Befehl **IOCControl.sh** muss als Benutzer ibmadmin ausgeführt werden. Sind Sie nicht als ibmadmin angemeldet, wechseln Sie mit dem Befehl **su - ibmadmin** zum Benutzeraccount ibmadmin.

Vorgehensweise

Führen Sie auf dem Verwaltungsserver den folgenden Befehl aus, um den Status aller IBM Intelligent Operations Center-Services abzufragen.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status all Kennwort
```

Hierbei ist *Kennwort* das Kennwort für das Plattformsteuerungstool, das bei der Installation von Plattformsteuerungstool definiert wurde.
Führen Sie den folgenden Befehl aus, um nur einen Service zu überprüfen.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status Service-ID Kennwort
```

Hierbei ist *Service-ID* eine Kennung, die unter **Zieloptionen** im Hilfetext von **IOCControl** aufgelistet ist, und *Kennwort* das Kennwort für das Plattformsteuerungstool, das bei der Installation von Plattformsteuerungstool definiert wurde.

Ergebnisse

Für gestartete Services wird **[on]** angezeigt. Für nicht gestartete Services wird **[off]** angezeigt.

Nächste Schritte

Überprüfen Sie nach der Ausführung des Befehls **IOCControl.sh** die Protokolle im Verzeichnis /opt/IBM/ISP/mgmt/logs. Diese Protokolle enthalten das Ergebnis der Ausführung von **IOCControl.sh**.

Zugehörige Tasks:

„Services starten” auf Seite 206
Zum Starten von Services, die auf IBM Intelligent Operations Center-Servern ausgeführt werden, ist das Plattformsteuerungstool verfügbar.

„Services stoppen” auf Seite 209
Zum Stoppen von IBM Intelligent Operations Center-Services ist das Plattformsteuerungstool verfügbar.

„Hilfe für das Plattformsteuerungstool abrufen”
Es sind Informationen zu Aktions- und Zieloptionen für das Plattformsteuerungstool verfügbar.

„Plattformsteuerungstool installieren” auf Seite 53
Das Plattformsteuerungstool wird verwendet, um die Serverumgebung von IBM Intelligent Operations Center zu verwalten. Das Tool wird getrennt vom Produkt installiert.

Hilfe für das Plattformsteuerungstool abrufen

Es sind Informationen zu Aktions- und Zieloptionen für das Plattformsteuerungstool verfügbar.

Informationen zu diesem Vorgang

Der Befehl **IOCControl.sh** muss als Benutzer `ibmadmin` ausgeführt werden. Sind Sie nicht als `ibmadmin` angemeldet, wechseln Sie mit dem Befehl **su - ibmadmin** zum Benutzeraccount `ibmadmin`.

Vorgehensweise

Führen Sie auf dem Verwaltungsserver einen der folgenden Befehle aus, um Optionen für den Befehl **IOCControl** anzuzeigen.

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh help
```

oder

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh
```

Ergebnisse

Die Optionen für den Befehl **IOCControl** werden angezeigt.

Zugehörige Tasks:

„Services starten” auf Seite 206
Zum Starten von Services, die auf IBM Intelligent Operations Center-Servern ausgeführt werden, ist das Plattformsteuerungstool verfügbar.

„Services stoppen” auf Seite 209
Zum Stoppen von IBM Intelligent Operations Center-Services ist das Plattformsteuerungstool verfügbar.

„Status der Services abfragen” auf Seite 212
Das Plattformsteuerungstool ist für die Bestimmung des Status von IBM Intelligent Operations Center-Services verfügbar.

Administrationskonsolen

Mit dem Portlet "Administrationskonsolen" können Sie die Services verwalten, die von der Lösung bereitgestellt werden.

Rufen Sie das Portlet "Administrationskonsolen" auf, indem Sie in der WebSphere Portal-Verwaltungsschnittstelle auf "**Intelligent Operations** > **Administration Tools** > **Administration Consoles** (Intelligent Operations > Verwaltungstools > Administrationskonsolen)" klicken.

Für jeden Service können über Links im Portlet "Administrationskonsolen" entweder eine Administrationskonsole oder weitere Informationen zum Zugriff auf die Administration aufgerufen werden.

Anmerkung: Wenn Sie Microsoft Internet Explorer Version 8.0 verwenden, kann es vorkommen, dass beim Aufruf des Links für die Berichtsadministration ein Fehler auftritt. Die Nachricht lautet wie folgt: `Angeforderte Ressource nicht gefunden`. Sie können dieses Problem lösen, indem Sie die URL im Adressfeld des Browsers bearbeiten und zwischen dem Hostnamen und `/ServletGateway` die Zeichenfolge `/cognos` einfügen.

Anwendungsserver

Tabelle 74. Administration auf dem Anwendungsserver

Konsole	Administration
Anwendungsserver	Rufen Sie zur Verwaltung der verschiedenen Services, die vom IBM Intelligent Operations Center bereitgestellt werden, den Link für die webbasierte Konsole von WebSphere Application Server auf. Sie können die Server steuern, Ressourcen und Service-Provider verwalten sowie den Host und sonstige Umgebungseinstellungen ändern.
Berichtsadministration	Rufen Sie zur Einrichtung von Berichten den Link zu der webbasierten Konsole für IBM Cognos Connection auf. Sie können neue Berichte erstellen oder bereits vorhandene Berichte ändern. Außerdem können Sie Datenquellen konfigurieren, öffentliche und private Ordner einrichten, Berechtigungen und die Verteilung definieren und in einem Zeitplan die automatische Ausführung von Berichten festlegen.

Datenserver

Tabelle 75. Administration auf dem Datenserver

Konsole	Administration
Datenbank	Rufen Sie den Link zum Information Center auf, um nähere Informationen über die Verwaltung der Datenbank mit DB2 Enterprise Server Edition zu erhalten. Die Ausführung von Tasks kann in der grafischen Benutzerschnittstelle der Datenbanksteuerzentrale oder über die Befehlszeile erfolgen.

Ereignisserver

Tabelle 76. Administration auf dem Ereignisserver

Konsole	Administration
Kontakt	Rufen Sie zur Anzeige der aktuellen Einstellungen in der Datenbank "names.nsf" den Link zu der webbasierten Konsole für Lotus Domino Server auf. Mit der Datenbank "names.nsf" wird Lotus Domino Server konfiguriert. Konfigurationsänderungen können mit Domino Administration Client vorgenommen werden.
Administration der Ansprechpartner	Rufen Sie den Link zum Information Center auf, um nähere Informationen über den Download und die Einrichtung der Domino Administration Client for Lotus Domino-Funktion für die Verwaltung von Ansprechpartnern zu erhalten.

Tabelle 76. Administration auf dem Ereignisserver (Forts.)

Konsole	Administration
Ereignisbehandlung	Rufen Sie zur Verwaltung der Ereignisbehandlung mit der grafischen Benutzerschnittstelle des Objektservers den Link zu der webbasierten Konsole für Tivoli Netcool/OMNIbus auf.
Ereignisverarbeitung und -erweiterung	Rufen Sie zur Verwaltung der Ereignisverarbeitung den Link zu der webbasierten Konsole für Tivoli Netcool/ Impact auf. Sie können beispielsweise Datenbankverbindungen, Datenquellenverbindungen, die Einleitung von Ereignisprozessen, den Richtlinienstatus und Protokolle überprüfen.
Instant-Messaging-Server	Rufen Sie zur Verwaltung von Instant Messaging den Link zu der webbasierten Konsole für Lotus Sametime Community Server auf.
Nachrichtenbus	Rufen Sie den Link zum Information Center auf, um nähere Informationen über die Prüfung des Nachrichtenstatus mit WebSphere Message Broker zu erhalten.
Standard Operating Procedure-Administration	Rufen Sie den Link zu der webbasierten Konsole für Tivoli Service Request Manager Start Center auf, um Ressourcen und Standard Operating Procedures zu definieren. Sie können verfügbare Ressourcen und Aktivitäten für das Ereignismanagement im IBM Intelligent Operations Center definieren.
Standard Operating Procedure-Anwendungsserver	Rufen Sie zur Verwaltung den Link zu der webbasierten Konsole für den WebSphere Application Server auf, der Tivoli Service Request Manager bereitstellt.

Verwaltungsserver

Tabelle 77. Administration auf dem Verwaltungsserver

Konsole	Administration
Anwendungsüberwachung	Rufen Sie zur Verwaltung der Anwendungsüberwachung den Link zu der webbasierten Konsole für Tivoli Monitoring auf. Mit dieser Konsole können Sie Überprüfungen des Systemzustands durchführen.
Anwendungsserver für Verwaltung	Rufen Sie zur Verwaltung von integrierten Anwendungen den Link zu der webbasierten Konsole für WebSphere Application Server auf. Diese Administration umfasst auch die Verwaltung von Sicherheitsfunktionen in Verbindung mit Tivoli Access Manager und WebSEAL.
Datenbank	Rufen Sie den Link zum Information Center auf, um nähere Informationen über die Verwaltung der Datenbank mit DB2 Enterprise Server Edition zu erhalten. Die Ausführung von Tasks kann in der grafischen Benutzerschnittstelle der Datenbanksteuerzentrale oder über die Befehlszeile erfolgen.
Verzeichnis	Stellen Sie zur Verwaltung des Benutzerverzeichnisdienstes eine Verknüpfung zur webbasierten Konsole von Tivoli Directory Server her. Informationen zur Verwendung der webbasierten Tivoli Directory Server-Konsole erhalten Sie über den Link zum Information Center.

Portlet "Administrationskonsolen" anpassen

Sie haben die Möglichkeit, dieses Portlet anzupassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Zugehörige Verweise:

„Einstellungen des Administrationskonsolen-Portlet" auf Seite 155
Anpassen des Administrationskonsolen-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Zugehörige Informationen:

Information Center für IBM Lotus Domino und Notes

Information Center für IBM DB2-Datenbanken

Information Center für IBM Tivoli Directory Server

Services verwalten

Das Portlet Administrationskonsolen stellt Links zu Positionen bereit, an denen Sie die von der Lösung bereitgestellten Services verwalten können oder weitere Informationen über die Verwaltung der Services finden.

Anwendungsserver
Service des Anwendungsservers

Sie können eine Vielzahl von Tasks im Bereich Anwendungsmanagement auf einer allgemeinen webbasierten Konsole ausführen, der Integrated Solutions Console:

- Den Status des Servers überprüfen.
- Server und Cluster starten und stoppen.
- Anwendungen oder Patches implementieren.
- Die Liste verfügbarer Portlets verwalten.
- Die Services überwachen.
- Mit Anwendungsservicerichtlinien arbeiten.
- Service-Provider einschließlich REST-Service-Provider verwalten.
- Ressourcen verwalten.
- Die Sicherheit Ihrer Anwendungen verwalten.
- Mit virtuellen Hosts und anderen Umgebungseinstellungen arbeiten.
- Die Systemverwaltung durchführen.
- Die Serviceintegration verwalten.
- Den HTTP-Server verwalten.
- Die Protokollierung und Traceerstellung verwalten.

Weitere Informationen zum Anwendung-Service finden Sie in der Onlinehilfe für die Integrated Solutions Console oder über den Link zum Information Center für WebSphere Application Server am Ende des Abschnitts über Anwendungsserver.

Administrationsservice für Berichte

Für alle Tasks, die mit der Bereitstellung von Berichten in IBM Intelligent Operations Center zusammenhängen, können Sie die webbasierte Konsole für die Berichtsadministration verwenden:

- Datenquellen einrichten.

- Berichte erstellen, bearbeiten und löschen.
- Den Zugriff auf Berichte verwalten.
- Berichte planen.
- Die Verteilung von Berichten einrichten.

Weitere Informationen zum Berichtsadministration-Service erhalten Sie über den Link zum Informationen Center für IBM Cognos Business Intelligence am Ende des Abschnitts über Anwendungsserver.

Zugehörige Informationen:

Information Center für WebSphere Application Server Version 7.0

Information Center für IBM Cognos Business Intelligence

Datenserver

Datenbankservice

Sie können die IBM Intelligent Operations Center-Datenbanken über die Datenbankserviceinstanzen verwalten, die auf dem Datenserver gehostet werden. Eine Datenbankserviceinstanz ist ein getrennter, unabhängiger Prozess, der auf einem Server ausgeführt wird. Eine Instanz kann als Host für mehrere Datenbanken dienen. Jeder Instanz ist ein *Instanzname* zugewiesen. Folgende Instanzen werden auf dem Datenserver gehostet:

Tabelle 78. Datenbankinstanzen, die auf dem Datenserver gehostet werden

Instanz	Verwendet von
dsrdbm01	Verzeichnis-Service
db2inst1	Für Lösungen reserviert
db2inst2	Portalserver
db2inst3	Berichtsadministration
db2inst4	Geschäftsregeln und Geschäftsüberwachung-Service
db2inst5	Semantikmodell-Services
db2inst6	SOPs – Administration-Service
db2inst7	Identitätsmanagement-Service
db2inst8	Für Anwendungen reserviert

So verwalten Sie eine Instanz über ein Terminalfenster:

1. Melden Sie sich als Benutzer für *Instanzname* an.
2. Führen Sie den Befehl **db2** aus, um in den Befehlsmodus zu wechseln.
3. Geben Sie **?** ein, um eine Liste aller verfügbaren Befehle anzuzeigen. Für viele Befehle ist eine aktive Verbindung zu einer Datenbank erforderlich.
   - Um die verfügbaren Datenbanken für eine Instanz anzuzeigen, führen Sie den Befehl zum Auflisten des Datenbankverzeichnisses **list database directory** aus.
   - Führen Sie zum Herstellen einer Verbindung zu einer Datenbank den Befehl **connect to** *Datenbankname* aus.
4. Um die Verbindung zu einer Datenbank zu trennen und den Befehlsmodus mit Bedienerführung zu beenden, führen Sie den Befehl **terminate** aus.

Weitere Informationen zum -Datenbank-Service erhalten Sie über den Link zum Information Center für DB2-Datenbanken am Ende des Abschnitts über Datenserver.

Zugehörige Informationen:

Information Center für IBM DB2-Datenbanken

Ereignisserver

Ansprechpartner, Administration der Ansprechpartner und Instant Messaging-Services

Sie können Ansprechpartner, Administration der Ansprechpartner, Instant Messaging-Services mit folgenden Möglichkeiten verwalten:

- Lotus Domino-Serverkonsole, um Ihre aktuellen Ansprechpartner anzuzeigen.
- Lotus Domino Administration- Client, um die einmalige Anmeldung (Single Sign-On) zu konfigurieren und den Instant-Messaging-Server sowie den Lotus Sametime Client zu verwalten.
- Lotus Sametime Community-Server, um die Verfügbarkeit des Instant-Messaging-Servers zu protokollieren und zu überprüfen.

Anmerkung: Ansprechpartner, die auf der Lotus Domino-Serverkonsole angezeigt werden, gelten nur für das Kontakt-Portlet und stimmen nicht mit den IBM Intelligent Operations Center-Benutzern überein.

Weitere Informationen über Ansprechpartner, Administration der Ansprechpartner und Instant Messaging-Services erhalten Sie über den Link zum Information Center für Lotus Domino und Notes am Ende des Abschnitts über Ereignisserver.

Ereignisverarbeitungsservice

Sie können die Ereigniserfassung und -speicherung im IBM Intelligent Operations Center über die grafische Benutzerschnittstelle des Tivoli Netcool/OMNIbus-Objektservers verwalten.

1. Öffnen Sie eine Terminalsitzung mit aktiviertem X Window System.
2. Melden Sie sich als Root beim Server an.
3. Gehen Sie zum Verzeichnis `/opt/IBM/netcool/omnibus`.
4. Führen Sie zum Öffnen der Anwendung mit grafischer Benutzerschnittstelle den Befehl `bin/nco_config` aus.

Weitere Informationen zum Service zur Ereignisverarbeitung erhalten Sie über den Link zum Information Center für Tivoli Netcool/Impact am Ende des Abschnitts über Ereignisserver.

Service zur Ereignisverarbeitung und -erweiterung

Sie können die Ereignisverarbeitung über die webbasierte Konsole für Tivoli Netcool/Impact verwalten:

- Überprüfen Sie die Datenbank- und die Datenquellenverbindungen.
- Überprüfen Sie, ob der Ereignisprozessor ausgeführt wird.
- Überprüfen Sie die Protokollierung für bereits vorhandene Richtlinien und aktualisieren Sie die Protokollebene.
- Aktualisieren Sie bereits vorhandene Richtlinien oder erstellen Sie neue Richtlinien.

Weitere Informationen zum Service zur Ereignisverarbeitung und -erweiterung erhalten Sie über den Link zum Information Center für Tivoli Netcool/Impact am Ende des Abschnitts über Ereignisserver.

Nachrichtenbus

Die drei Hauptmethoden zur Verwaltung des Service für den Nachrichtenbus lauten wie folgt:

- Befehlszeile
- Explorer: eine Eclipse-basierte Verwaltungsanwendung

- Toolkit: eine Eclipse-basierte Anwendung, mit der sowohl die Administration als auch die Anwendungsentwicklung möglich sind

Mit dem Entwicklungstool für grafische Benutzerschnittstellen können Sie Kommunikationsabläufe verwalten sowie Tests, Transformationen, Integrationen und die Protokollierung definieren.

Das WebSphere Message Broker-Toolkit wird mit dem IBM Intelligent Operations Center bereitgestellt. Weitere Informationen zur Installation und Verwendung des Toolkits erhalten Sie über den Link zum Information Center für WebSphere Message Broker am Ende des Abschnitts über Ereignisserver.

So konfigurieren Sie eine Befehlszeilenumgebung und fragen WebSphere Message Broker-Instanzen ab:

- Melden Sie sich als Benutzer `mqm` beim Server an.
- Gehen Sie zum Verzeichnis `/opt/IBM/mqsi/8.0.0.0`.
- Führen Sie zum Konfigurieren der Umgebung den Befehl `source bin/mqsiprofile` aus.
- Führen Sie zum Abfragen der WebSphere Message Broker-Instanzen den Befehl `bin/mqsilist` aus.

Weitere Informationen zum Nachrichtenbus-Service erhalten Sie über den Link zum Information Center für WebSphere Message Broker am Ende des Abschnitts über Ereignisserver.

Standard Operating Procedure-Administrationsservice

Sie können Ressourcen und Aktivitäten zur Verwaltung von Ereignissen über die webbasierte SOPs – Administration-Konsole, das Tivoli Service Request Manager-Startcenter definieren.

Weitere Informationen zum SOPs – Administration-Service erhalten Sie über den Link zum Information Center für Tivoli Service Request Manager am Ende des Abschnitts über Ereignisserver.

Standard Operating Procedure-Anwendungsservice

Sie können Anwendungen, die zu Ressourcen und Aktivitäten gehören, über die webbasierte Konsole für WebSphere Application Server verwalten, auf dem Tivoli Service Request Manager ausgeführt wird.

Weitere Informationen zum Standard Operating Procedure-Anwendungsservice erhalten Sie in der Onlinehilfe oder über den Link zum Information Center für WebSphere Application Server Version 7.0 am Ende des Abschnitts über Anwendungsserver.

Zugehörige Konzepte:

„Tivoli Service Request Manager konfigurieren” auf Seite 131
In der Benutzerschnittstelle von Tivoli Service Request Manager können Sie Standard Operating Procedures, Workflows und Ressourcen verwalten.

Zugehörige Informationen:

Information Center für IBM Lotus Domino und Notes

Information Center für IBM Tivoli Netcool/Impact

Information Center für IBM WebSphere Message Broker

Information Center für IBM Tivoli Service Request Manager

Verwaltungsserver

Anwendungsüberwachungsservice

Sie können die Anwendungsüberwachung über die webbasierte Konsole für Tivoli Monitoring verwalten. Laden Sie die Anwendung herunter und führen Sie sie aus, um den Status der Server zu überprüfen und alle ausgeführten Überwachungsagenten anzuzeigen. Geben Sie zum Anmelden Ihre Benutzer-ID und Ihr

Kennwort ein. Die Standard-Benutzer-ID lautet "sysadmin", und als Kennwort verwenden Sie das während der Installation eingegebene Topologiekennwort.

Weitere Informationen zum Anwendungsüberwachungsservice erhalten Sie über den Link zum Benutzerhandbuch für Tivoli Enterprise Portal am Ende des Themas.

Anwendungsserver für Management-Service

Sie können Junctions für Tivoli Access Manager WebSEAL auf der allgemeinen webbasierten Konsole, der Integrated Solutions Console, verwalten.

Weitere Informationen zu diesem Service erhalten Sie in der Onlinehilfe oder über den Link zum Information Center für WebSphere Application Server Version 7.0 am Ende des Abschnitts über Anwendungsserver.

Datenbankservice

Auf dem Management-Server wird eine -Datenbank-Serviceinstanz, `db2inst2`, gehostet. Sie können diese Instanz für das Systemmanagement und für bestimmte Datenspeichervorgänge für Tivoli Access Manager verwenden.

Weitere Informationen zum -Datenbankservice erhalten Sie über den Link zum Information Center für IBM DB2-Datenbanken am Ende des Abschnitts über Datenserver.

Verzeichnisservice

Wenn Sie das Benutzerverzeichnis über die webbasierte Konsole für Tivoli Directory Server verwalten, können Sie Benutzer in LDAP anzeigen, hinzufügen oder ändern.

Weitere Informationen zum Verzeichnisservice erhalten Sie über den Link zum Information Center für Tivoli Directory Server am Ende dieses Themas.

Zugehörige Informationen:

 Benutzerhandbuch für IBM Tivoli Monitoring, Tivoli Enterprise Portal

 Information Center für IBM Tivoli Directory Server

---

Komponenten überprüfen

Mit dem Systemprüfungstool wird überprüft, ob auf die Komponenten in IBM Intelligent Operations Center zugegriffen werden kann und ob sie betriebsbereit sind.

Verwendung des Systemprüfungtools

Das Systemprüfungstool wird zum Ermitteln des Betriebsstatus von Services verwendet, aus denen sich das IBM Intelligent Operations Center-System zusammensetzt.

Informationen zu diesem Vorgang

Mit dem Systemprüfungstool werden die Systemfunktionen überprüft.

Wenn Sie Details zu den einzelnen Tests abrufen möchten sowie zur Fehlerbestimmung, falls ein Test fehlschlägt, klicken Sie für den betreffenden Test auf **Hilfe**.

Über **Eigenschaften** können Sie weitere Informationen zum Test anzeigen, die hilfreich sind, wenn Sie sich mit IBM Software Support in Verbindung setzen.

Vorgehensweise

1. Melden Sie sich an IBM Intelligent Operations Center als Benutzer mit Administratorberechtigung an.
2. Klicken Sie auf **Intelligent Operations** > **Administration Tools** > **System Verification Check** (Intelligent Operations > Verwaltungstools > Systemprüfung).
3. Wählen Sie den Test bzw. die Tests aus, die ausgeführt werden sollen; Sie haben folgende Möglichkeiten:
   - Klicken Sie auf den Test, der ausgeführt werden soll.
   - Klicken Sie auf **Alle Tests ausführen**, um die Funktionen der gesamten Auswahl zu überprüfen.

Ergebnisse

Das Symbol  wird angezeigt, wenn ein Test erfolgreich abgeschlossen wurde. Das Symbol  wird angezeigt, wenn ein Test fehlschlägt. Schlägt ein Test fehl, gehen Sie entsprechend den Anweisungen zur Fehlerbestimmung für den Test vor, um die Fehler zu beheben. Diese Anweisungen können auch durch Klicken auf das Symbol  oder auf **Hilfe** aufgerufen werden.

Bei Ausführung eines bestimmten Tests werden die Ergebnisse dieser Testausführung zusammen mit der Ausführungsdauer unten im Portlet angezeigt. Bei Auswahl von **Alle Tests ausführen** werden diese Informationen nicht angezeigt.

Nächste Schritte

Durch Klicken auf **Zurücksetzen** wird das Tool zurückgesetzt; damit werden alle Ergebnisse gelöscht.

Zugehörige Tasks:

„Installation überprüfen” auf Seite 55
Überprüfen Sie nach der Installation von IBM Intelligent Operations Center dass das Produkt ordnungsgemäß installiert wurde.

„Das Tool Systemprüfung installieren” auf Seite 54
Das Tool Systemprüfung wird verwendet, um den Betriebsstatus von Komponenten in IBM Intelligent Operations Center zu überprüfen. Das Tool wird getrennt vom Produkt installiert.

Systemprüfungen

In IBM Intelligent Operations Center stehen eine Reihe von Systemprüfungen bereit, mit deren Hilfe der Betriebsstatus verschiedener IBM Intelligent Operations Center-Services und -Komponenten überprüft werden kann.

Diese Tests sind nach Funktion zusammengefasst, beispielsweise Zusammenarbeit und Überwachung.

Test "Account Management (Tivoli Identity Manager API)"

Mit dem Test "Account Management (Tivoli Identity Manager API)" wird der Zugriff auf die Tivoli Identity Manager-API über den IIOP-Port geprüft.

Ressourcen

Für den Test "Account Management (Tivoli Identity Manager API)" wird die folgende Ressource verwendet:

- Tivoli Identity Manager-Server (auf dem Verwaltungsserver).

Fehlerbestimmung

Schlägt der Test "Account Management (Tivoli Identity Manager API)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem Anwendungsserver und dem Verwaltungsserver eine Netzverbindung besteht. Dazu können vom Anwendungsserver aus **ping**-Befehle mit dem kurzen und dem vollständig qualifizierten Hostnamen des Verwaltungsservers gesendet werden. Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Verwaltungsserver die folgenden Tivoli Identity Manager-Protokolle:
      - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log`
      - Alle Protokolle in V6-Unterverzeichnissen des Verzeichnisses `/var/idsldap/`
3. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Anwendungsserver und auf dem Verwaltungsserver erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
4. Überprüfen Sie, ob der Tivoli Identity Manager-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:
   a. Melden Sie sich auf dem Verwaltungsserversystem als `ibmadmin` an.
   b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password` *WAS-Administratorkennwort* aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh`. Wird die Nachricht `ADMU0508I: The Application Server "nodeagent" is STARTED.` (Der Anwendungsserver "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server nodeagent open for e-business; process id is 26654` (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).
   a. Wird die Nachricht `ADMU0509I: The Application Server "timServer1" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "timServer1" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1`. Wird die Nachricht `ADMU0508I: The Application Server "timServer1" is STARTED.` (Der Anwendungsserver "timServer1" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "timServer1" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server timserver open for e-business; process id is 26654` (Server "timeserver" verfügbar für E-Business; Prozess-ID ist 26654).

   Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

   Starten Sie die Server in der folgenden Reihenfolge:
   a. nodeagent
   b. timServer1

   Stoppen Sie die Server in der folgenden Reihenfolge:
   a. timServer1

b. nodeagent

Der Server "timServer1" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Verwaltungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

5. Überprüfen Sie, ob der Tivoli Identity Manager-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung mithilfe der Administrationskonsole von WebSphere Application Server durch:
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://`*`Managementserver-Host`*`:9060/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Verwaltungsserver-Host* ist der Hostname für den Verwaltungsserver.
   b. Überprüfen Sie den Status des Servers "timServer1", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

      Das Symbol  zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

      Das Symbol  zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

      Das Symbol  zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Knotenagent (nodeagent) unter Umständen nicht aktiv. Sie können den Knotenagenten starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh` ausführen.

   Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

   Starten Sie die Server in der folgenden Reihenfolge:
   a. nodeagent
   b. timServer1

   Stoppen Sie die Server in der folgenden Reihenfolge:
   a. timServer1
   b. nodeagent

   Um den Server "timServer1" zu stoppen, wählen Sie den Server aus und klicken Sie auf die entsprechende Option.

   Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Verwaltungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.
6. Überprüfen Sie, ob der Zugriff auf die Tivoli Identity Manager-Konsole vom WebSphere Portal-System auf dem Anwendungsserver über die URL `http://`*`Verwaltungsserver-Host`*`:9080/itim/console/main` aus möglich ist; Dabei steht *Verwaltungsserver-Host* für den Hostnamen des Verwaltungsservers. Melden Sie sich mit der Benutzer-ID `itim manager` an.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Account Management (Tivoli Identity Manager Console)"

Mit dem Test "Account Management (Tivoli Identity Manager Console)" wird festgestellt, ob der Zugriff auf Tivoli Identity Manager über die Tivoli Identity Manager-Verwaltungs-URL möglich ist.

Ressourcen

Für den Test "Account Management (Tivoli Identity Manager Console)" wird die folgende Ressource verwendet:

- Tivoli Identity Manager-Server (auf dem Verwaltungsserver)

Fehlerbestimmung

Schlägt der Test "Account Management (Tivoli Identity Manager Console)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem Anwendungsserver und dem Verwaltungsserver eine Netzverbindung besteht. Dazu können vom Anwendungsserver aus **ping**-Befehle mit dem kurzen und dem vollständig qualifizierten Hostnamen des Verwaltungsservers gesendet werden. Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Verwaltungsserver die folgenden Tivoli Identity Manager-Protokolle:
      - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log`
      - Alle Protokolle in V6-Unterverzeichnissen des Verzeichnisses `/var/idsldap/`
3. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Anwendungsserver und auf dem Verwaltungsserver erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
4. Überprüfen Sie, ob der Tivoli Identity Manager-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:
   a. Melden Sie sich auf dem Verwaltungsserversystem als `ibmadmin` an.
   b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password` *`WAS-Administratorkennwort`* aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh`. Wird die Nachricht `ADMU0508I: The Application Server "nodeagent" is STARTED.` (Der Anwendungsserver "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server nodeagent open for e-business; process id is 26654` (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).
   a. Wird die Nachricht `ADMU0509I: The Application Server "timServer1" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "timServer1" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1`. Wird die Nachricht `ADMU0508I: The Application Server "timServer1" is STARTED.` (Der Anwen-

dungsserver "timServer1" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "timServer1" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server timserver open for e-business; process id is 26654` (Server "timeserver" verfügbar für E-Business; Prozess-ID ist 26654).

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. timServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. timServer1
b. nodeagent

Der Server "timServer1" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Verwaltungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

5. Überprüfen Sie, ob der Tivoli Identity Manager-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung mithilfe der Administrationskonsole von WebSphere Application Server durch:
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://`*`Managementserver-Host`*`:9060/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Verwaltungsserver-Host* ist der Hostname für den Verwaltungsserver.
   b. Überprüfen Sie den Status des Servers "timServer1", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

      Das Symbol  zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

      Das Symbol  zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

      Das Symbol  zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Knotenagent (nodeagent) unter Umständen nicht aktiv. Sie können den Knotenagenten starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh` ausführen.

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. timServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. timServer1
b. nodeagent

Um den Server "timServer1" zu stoppen, wählen Sie den Server aus und klicken Sie auf die entsprechende Option.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Verwaltungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS-Administratorkennwort` ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

6. Überprüfen Sie, ob der Zugriff auf die Tivoli Identity Manager-Konsole vom WebSphere Portal-System auf dem Anwendungsserver über die URL `http://Verwaltungsserver-Host:9080/itim/console/main` aus möglich ist; Dabei steht *Verwaltungsserver-Host* für den Hostnamen des Verwaltungsservers. Melden Sie sich mit der Benutzer-ID `itim manager` an.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Account Management (Tivoli Directory Integrator list assembly)"

Mit dem Test "Account Management (Tivoli Directory Integrator list assembly)" wird festgestellt, ob die Tivoli Directory Integrator List Assembly-Ressourcen verfügbar sind. Dazu wird auf dem Verwaltungsserver der Befehl **tdisrvctl** für die Remote-Verwaltung von Konfigurationen, AssemblyLines und anderen Funktionen ausgeführt; bei dem Test wird geprüft, ob die Zeichenfolge `"--- AssemblyLines ---"` zurückgegeben wird.

Ressourcen

Für den Test Account Management (Tivoli Directory Integrator list assembly)" werden die folgenden Ressourcen verwendet:

- Tivoli Directory Server (auf dem Datenserver)
- Tivoli Directory Integrator (auf dem Verwaltungsserver)

Fehlerbestimmung

Schlägt der Test "Account Management (Tivoli Directory Integrator list assembly)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem Anwendungsserver und dem Datenserver eine Netzverbindung besteht. Dazu können vom Anwendungsserver aus **ping**-Befehle mit dem kurzen und dem vollständig qualifizierten Namen des Datenservers gesendet werden. Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Überprüfen Sie, ob die Kapazität der Dateisysteme auf den Datenserver- und Anwendungsserversystemen erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
4. Überprüfen Sie, ob der Tivoli Directory Integrator-Server aktiv ist.
   a. Melden Sie sich auf dem Verwaltungsserver als `ibmadmin` an einer Terminalsitzung an.
   b. Führen Sie den Befehl **ps -ef | grep ibmdisrv** aus. Das Ergebnis ist ähnlich dem folgenden Beispiel:

```
ibmadmin      11411      1  0 Sep06 pts/1     00:00:00 /bin/sh /opt/IBM/TDI/V7.1/ibmdisrv -s /opt/IBM/TDI/V7.1/timsol -c ITIM_RMI.xml -d
ibmadmin      32080 19149  0 23:17 pts/1     00:00:00 grep ibmdisrv
```

   Aus diesem Beispiel geht hervor, dass der Tivoli Directory Integrator-Serverdämon "ibmdisrv" aktiv ist.
5. Ist der Tivoli Directory Integrator-Server "ibmdisrv" nicht aktiv, starten Sie den Server.

a. Melden Sie sich auf dem Verwaltungsserver als `root` an einer Terminalsitzung an.
b. Führen Sie `/etc/init.d/ITIMAd start` aus.

6. Überprüfen Sie, ob der LDAP-Server von Tivoli Directory Server aktiv ist.
   a. Melden Sie sich auf dem Datenserver als `root` an einer Terminalsitzung an.
   b. Führen Sie den Befehl **ps -ef | grep ibmslapd** aus. Das Ergebnis ist ähnlich dem folgenden Beispiel:

      ```
      dsrdbm01 13797     1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
      root     32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
      ```

      Aus diesem Beispiel geht hervor, dass der Tivoli Directory Server-Dämon "ibmslapd" aktiv ist.
   c. Führen Sie den Befehl **ps -ef | grep ibmdiradm** aus. Das Ergebnis ist ähnlich dem folgenden Beispiel:

      ```
      root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
      dsrdbm01 11055     1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
      ```

      Aus diesem Beispiel geht hervor, dass der Tivoli Directory Server-Dämon "ibmdiradm" aktiv ist.
7. Ist der Tivoli Directory Server "ibmslapd" nicht aktiv, gehen Sie wie folgt vor:
   a. Melden Sie sich als Linux-Benutzer *root* an, und führen Sie den Befehl **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** aus, um Directory Server zu starten.
8. Ist der Tivoli Directory-Administrationsserver "ibmdiradm" nicht aktiv, gehen Sie wie folgt vor:
   a. Führen Sie in einer Terminalsitzung auf dem Datenserver den Befehl **su - dsrdbm01** aus.
   b. Führen Sie den Befehl **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** aus, um den Anwendungsserver zu starten.
9. Ist der Tivoli Directory Server "ibmslapd" aktiv, gehen Sie wie folgt vor:

   Anmerkung: Führen Sie diesen Schritt auch dann aus, wenn Tivoli Directory Server im vorangegangenen Schritt gestartet wurde.
   a. Melden Sie sich auf dem Datenserver als "dsrdbm01" an einer Terminalsitzung an.
   b. Führen Sie den Befehl **idsldapsearch -h localhost -D "cn=root" -w "***Administratorkennwort***" -s sub uid=*** aus; dabei ist *Administratorkennwort* das Kennwort für den LDAP-Rootadministratoraccount. Die vorhandenen LDAP-Benutzerobjekte werden angezeigt.
10. Überprüfen Sie, ob das Tivoli Directory Server-Webverwaltungstool aktiv ist. Mit dem Tivoli Directory Server-Webverwaltungstool können Sie die LDAP-Instanz stoppen und starten, Benutzer oder Konten hinzufügen und Protokolldateien anzeigen.
    a. Melden Sie sich auf dem Verwaltungsserver als `ibmadmin` an einer Terminalsitzung an.
    b. Führen Sie auf dem Verwaltungsserver den Befehl **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password** *WAS-Administratorkennwort* aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators. Ist das Tool aktiv, wird eine Nachricht ähnlich der folgenden zurückgegeben:

       ```
       ADMU0508I: The Application Server "tdsServer" is STARTED
       ```

       (Anwendungsserver "tdsServer" wurde gestartet)

       Wird die folgende Nachricht zurückgegeben, muss der Server "tdsServer" gestartet werden:

       ```
       ADMU0509I: The Application Server "tdsServer" cannot be reached. It appears to be stopped.
       ```

       (Der Anwendungsserver "tdsServer" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.)
    c. Starten Sie den Server "tdsServer" mit dem Befehl **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer** . Der Server "tdsServer" wird gestartet und eine Nachricht ähnlich der folgenden angezeigt:

       ```
       ADMU3000I: Server tdsServer open for e-business; process id is 26654
       ```

       (Server "tdsServer" ist für E-Business verfügbar; Prozess-ID ist 26654)

11. Rufen Sie das Tivoli Directory Server-Webverwaltungstool unter `http://`*`Verwaltungsserver-Host`*`:9062/IDSWebApp/IDSjsp/Login.jsp` auf. Dabei steht *Verwaltungsserver-Host* für den Hostnamen des Verwaltungsservers.
12. Melden Sie sich mit dem LDAP-Rootadministratoraccount (cn=root) und dem entsprechenden Kennwort an. Der LDAP-Server muss den Namen *Datenbank_Directory_Server-Host*:389 haben. Dabei steht *Datenbank_Directory_Server-Host* für den Hostnamen des Datenservers.
13. Klicken Sie auf **Server Administration** > **Start/stop/reset server** (Serververwaltung > Server starten/stoppen/zurücksetzen). Der Status des LDAP-Servers wird angezeigt. Über diese Seite kann der LDAP-Server auch gestartet, gestoppt oder zurückgesetzt werden.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Account Management (Tivoli Directory Server)"

Mit dem Test "Account Management (Tivoli Directory Server)" wird festgestellt, ob Tivoli Directory Server verfügbar ist, indem eine HTTP-Anforderung an den Server gesendet wird.

Ressourcen

Für den Test "Account Management (Tivoli Directory Server)" wird die folgende Ressource verwendet:

- Tivoli Directory Server (auf dem Datenserver)

Fehlerbestimmung

Schlägt der Test fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Datenserver erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
3. Überprüfen Sie, ob der LDAP-Server von Tivoli Directory Server aktiv ist.
   a. Melden Sie sich auf dem Datenserver als `root` an einer Terminalsitzung an.
   b. Führen Sie den Befehl **ps -ef | grep ibmslapd** aus. Das Ergebnis ist ähnlich dem folgenden Beispiel:

      ```
      dsrdbm01 13797     1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
      root     32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
      ```

      Aus diesem Beispiel geht hervor, dass der Tivoli Directory Server-Dämon "ibmslapd" aktiv ist.
   c. Führen Sie den Befehl **ps -ef | grep ibmdiradm** aus. Das Ergebnis ist ähnlich dem folgenden Beispiel:

      ```
      root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
      dsrdbm01 11055     1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
      ```

      Aus diesem Beispiel geht hervor, dass der Tivoli Directory Server-Dämon "ibmdiradm" aktiv ist.
4. Ist der Tivoli Directory Server "ibmslapd" nicht aktiv, gehen Sie wie folgt vor:
   a. Melden Sie sich als Linux-Benutzer *root* an, und führen Sie den Befehl **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** aus, um Directory Server zu starten.
5. Ist der Tivoli Directory-Administrationsserver "ibmdiradm" nicht aktiv, gehen Sie wie folgt vor:
   a. Führen Sie in einer Terminalsitzung auf dem Datenserver den Befehl **su - dsrdbm01** aus.

b. Führen Sie den Befehl **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** aus, um den Anwendungsserver zu starten.

6. Ist der Tivoli Directory Server "ibmslapd" aktiv, gehen Sie wie folgt vor:

   Anmerkung: Führen Sie diesen Schritt auch dann aus, wenn Tivoli Directory Server im vorangegangenen Schritt gestartet wurde.

   a. Melden Sie sich auf dem Datenserver als "dsrdbm01" an einer Terminalsitzung an.
   b. Führen Sie den Befehl **idsldapsearch -h localhost -D "cn=root" -w "***Administratorkennwort***" -s sub uid=*** aus; dabei ist *Administratorkennwort* das Kennwort für den LDAP-Rootadministratoraccount. Die vorhandenen LDAP-Benutzerobjekte werden angezeigt.

7. Überprüfen Sie, ob das Tivoli Directory Server-Webverwaltungstool aktiv ist. Mit dem Tivoli Directory Server-Webverwaltungstool können Sie die LDAP-Instanz stoppen und starten, Benutzer oder Konten hinzufügen und Protokolldateien anzeigen.

   a. Melden Sie sich auf dem Verwaltungsserver als `ibmadmin` an einer Terminalsitzung an.
   b. Führen Sie auf dem Verwaltungsserver den Befehl **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password** *WAS-Administratorkennwort* aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators. Ist das Tool aktiv, wird eine Nachricht ähnlich der folgenden zurückgegeben:

      ```
      ADMU0508I: The Application Server "tdsServer" is STARTED
      ```

      (Anwendungsserver "tdsServer" wurde gestartet)

      Wird die folgende Nachricht zurückgegeben, muss der Server "tdsServer" gestartet werden:

      ```
      ADMU0509I: The Application Server "tdsServer" cannot be reached. It appears to be stopped.
      ```

      (Der Anwendungsserver "tdsServer" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.)

   c. Starten Sie den Server "tdsServer" mit dem Befehl **/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer** . Der Server "tdsServer" wird gestartet und eine Nachricht ähnlich der folgenden angezeigt:

      ```
      ADMU3000I: Server tdsServer open for e-business; process id is 26654
      ```

      (Server "tdsServer" ist für E-Business verfügbar; Prozess-ID ist 26654)

8. Rufen Sie das Tivoli Directory Server-Webverwaltungstool unter `http://`*`Verwaltungsserver-Host`*`:9062/IDSWebApp/IDSjsp/Login.jsp` auf. Dabei steht *Verwaltungsserver-Host* für den Hostnamen des Verwaltungsservers.
9. Melden Sie sich mit dem LDAP-Rootadministratoraccount (cn=root) und dem entsprechenden Kennwort an. Der LDAP-Server muss den Namen *`Datenbank_Directory_Server-Host`*`:389` haben. Dabei steht *Datenbank_Directory_Server-Host* für den Hostnamen des Datenservers.
10. Klicken Sie auf **Server Administration** > **Start/stop/reset server** (Serververwaltung > Server starten/stoppen/zurücksetzen). Der Status des LDAP-Servers wird angezeigt. Über diese Seite kann der LDAP-Server auch gestartet, gestoppt oder zurückgesetzt werden.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Analytics (Cognos Gateway Console)"

Mit dem Test "Analytics (Cognos Gateway Console)" wird festgestellt, ob über das Cognos-Servlet-Gateway und die Cognos Administration-Portal-URL auf Cognos auf dem Anwendungsserver zugegriffen werden kann.

Ressourcen

Für den Test "Analytics (Cognos Gateway Console)" wird die folgende Ressource verwendet:

- Cognos (auf dem Anwendungsserversystem).

Fehlerbestimmung

Schlägt der Test "Analytics (Cognos Gateway Console)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Zugriffsproblem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Anwendungsserver die folgenden Cognos-Protokolle:
      - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Disp1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Disp1/SystemErr.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemErr.log`
      - Alle Protokolle im Verzeichnis `/opt/IBM/cognos/c10_64/logs/`
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Anwendungsserversystem erreicht wurde (dies kann mit dem Befehl **`df -h`** festgestellt werden).
3. Prüfen Sie, ob der Cognos Dispatcher- und der Cognos Gateway-Server gestartet wurden. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:
   a. Melden Sie sich auf dem Anwendungsserversystem als `cgnsadm` (Cognos-Benutzer) an.
   b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *`WAS-Administratorkennwort`* aus; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "nodeagent" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh`. Wird die Nachricht `ADMU0508I: The Application Server "nodeagent" is STARTED.` (Der Anwendungsserver "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server nodeagent open for e-business; process id is 26654` (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).
   d. Wird die Nachricht `ADMU0509I: The Application Server "CognosX_Disp1" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "CognosX_Disp1" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "CognosX_Disp1" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX_Disp1`. Wird die Nachricht `ADMU0508I: The Application Server "CognosX_Disp1" is STARTED.` (Der Anwendungsserver "CognosX_Disp1" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie "CognosX_Disp1" starten mussten, wird eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server CognosX_Disp1 open for e-business; process id is 26654` (Server "CognosX_Disp1" ist für E-Business verfügbar; Prozess-ID ist 26654).
   e. Wird die Nachricht `ADMU0509I: The Application Server "CognosX_GW1" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "CognosX_GW1" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "CognosX_GW1" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX_GW1`. Wird

die Nachricht `ADMU0508I: The Application Server "CognosX_GW1" is STARTED.` (Der Anwendungsserver "CognosX_GW1" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie "CognosX_GW1" starten mussten, wird eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server CognosX_GW1 open for e-business; process id is 26676` (Server "CognosX_GW1" ist für E-Business verfügbar; Prozess-ID ist 26676).

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. CognosX_Disp1
c. CognosX_GW1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. CognosX_GW1
b. CognosX_Disp1
c. nodeagent

Der Server "CognosX_GW1" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX_GW1 -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "CognosX_Disp1" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX_Disp1 -wasadmin admin -password` *`WAS-Administratorkennwort`* ausgeführt wird; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

4. Prüfen Sie, ob der Cognos Dispatcher- und der Cognos Gateway-Server gestartet wurden. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung mithilfe der Administrationskonsole von WebSphere Application Server durch:
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://`*`Anwendungsserver-Host`*`:9060/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Anwendungsserver-Host* ist der Hostname für den Anwendungsserver.
   b. Überprüfen Sie den Status der Server "CognosX-Disp1" und "CognosX_GW1", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

      Das Symbol  zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

      Das Symbol  zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

      Das Symbol  zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Server "nodeagent" unter Umständen nicht aktiv. Sie können den Server "nodeagent" starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh` ausführen.

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. CognosX_Disp1
c. CognosX_GW1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. CognosX_GW1
b. CognosX_Disp1
c. nodeagent

Um die Server "CognosX_GW1" und "CognosX_Disp1" zu stoppen, wählen Sie die Server aus und klicken Sie auf die entsprechende Option.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

5. Überprüfen Sie, ob der Zugriff auf das Cognos Administration-Portal vom WebSphere Portal-System auf dem Anwendungsserver aus über die URL `http://`*`Anwendungsserver-Host`*`:9081/ServletGateway/servlet/Gateway` möglich ist; dabei ist *Anwendungsserver-Host* der Hostname für den Anwendungsserver.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Application Server (WebSphere Application Server Web Service)"

Mit dem Test "Application Server (WebSphere Application Server Web Service)" wird festgestellt, ob der Zugriff auf den WebSphere Application Server-Web-Service über den Web-Service "DrpGeoSvcs" möglich ist.

Ressourcen

Für den Test "Application Server (WebSphere Application Server Web Service)" wird die folgende Ressource verwendet:

- WebSphere Application Server (auf dem Anwendungsserver).

Fehlerbestimmung

Schlägt der Test "Application Server (WebSphere Application Server Web Service)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere-UDDI-Registry-Konfigurationsprotokolle:
      - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log`
2. Überprüfen Sie, ob die Kapazität des Dateisystems auf dem Anwendungsserver erreicht wurde (dies kann mit dem Befehl **`df -h`** festgestellt werden).
3. Überprüfen Sie, ob der Server "cpudServer1" gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:

a. Melden Sie sich auf dem Anwendungsserversystem als `ibmadmin` an.
b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *`WAS-Administratorkennwort`* aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
c. Wird die Nachricht `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh`. Wird die Nachricht `ADMU0508I: The Application Server "nodeagent" is STARTED.` (Der Anwendungsserver "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server nodeagent open for e-business; process id is 26654` (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).
a. Wird die Nachricht `ADMU0509I: The Application Server "cpudServer1" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "cpudServer1" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "cpudServer1" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1`. Wird die Nachricht `ADMU0508I: The Application Server "cpudServer1" is STARTED.` (Der Anwendungsserver "cpudServer1" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "cpudServer1" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server cpudServer1 open for e-business; process id is 26654` (Server "cpudServer1" für E-Business verfügbar, Prozess-ID ist 26654.)

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. cpudServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. cpudServer1
b. nodeagent

Der Server "cpudServer1" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

4. Überprüfen Sie, ob der Server "cpudServer1" gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung mithilfe der Administrationskonsole von WebSphere Application Server durch:
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://`*`Anwendungsserver-Host`*`:9060/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Anwendungsserver-Host* ist der Hostname für den Anwendungsserver.
   b. Überprüfen Sie den Status des Servers "cpudServer1", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

      Das Symbol zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

Das Symbol zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

Das Symbol zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Knotenagent (nodeagent) unter Umständen nicht aktiv. Sie können den Knotenagenten starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh` ausführen.

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. cpudServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. cpudServer1
b. nodeagent

Um den Server "cpudServer" zu stoppen, wählen Sie den Server aus und klicken Sie auf die entsprechende Option.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

5. Überprüfen Sie, ob ein Zugriff auf die WebSphere-UDDI-Benutzerkonsole möglich ist.
   a. Rufen Sie auf dem Anwendungsserver `https://`*`Anwendungsserver-Host`*`:9080/uddigui/` auf. Dabei steht *Anwendungsserver-Host* für den Hostnamen des Anwendungsservers.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Business Rules (WebSphere Operational Decision Manager JRules Console)"

Mit dem Test "Business Rules (WebSphere Operational Decision Manager JRules Console)" wird der Zugriff auf WebSphere Operational Decision Management JRules über die Rule Execution Server-Konsole überprüft.

Ressourcen

Für den Test "Business Rules (WebSphere Operational Decision Manager JRules Console)" wird die folgende Ressource verwendet:

- WebSphere Operational Decision Management JRules (auf dem Anwendungsserver).

Fehlerbestimmung

Schlägt der Test "Business Rules (WebSphere Operational Decision Manager JRules Console)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Operational Decision Management-Konfigurationsprotokolle:

- /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log
- /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log

2. Überprüfen Sie, ob die Kapazität des Dateisystems auf dem Anwendungsserver erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
3. Überprüfen Sie, ob Rule Execution Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:
   a. Melden Sie sich auf dem Anwendungsserversystem als ibmadmin an.
   b. Führen Sie in einem Befehlsfenster den Befehl /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password *WAS-Administratorkennwort* aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped. (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl /opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh. Wird die Nachricht ADMU0508I: The Application Server "nodeagent" is STARTED. (Der Anwendungsserver "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: ADMU3000I: Server nodeagent open for e-business; process id is 26654 (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).
   a. Wird die Nachricht ADMU0509I: The Application Server "wodmServer1" cannot be reached. It appears to be stopped. (Der Anwendungsserver "cpudServer1" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "wodmServer1" mit dem Befehl /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1. Wird die Nachricht ADMU0508I: The Application Server "wodmServer1" is STARTED. (Der Anwendungsserver "wodmServer1" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "wodmServer1" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: ADMU3000I: Server wodmServer1 open for e-business; process id is 26654 (Server "wodmServer1" ist für E-Business verfügbar; Prozess-ID ist 26654).

   Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

   Starten Sie die Server in der folgenden Reihenfolge:
   a. nodeagent
   b. wodmServer1

   Stoppen Sie die Server in der folgenden Reihenfolge:
   a. wodmServer1
   b. nodeagent

   Der Server "wodmServer1" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password *WAS-Administratorkennwort* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

   Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password *WAS-Administratorkennwort* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.
4. Überprüfen Sie, ob Rule Execution Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung mithilfe der Administrationskonsole von WebSphere Application Server durch:

a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://Anwendungsserver-Host:9060/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Anwendungsserver-Host* ist der Hostname für den Anwendungsserver.
b. Überprüfen Sie den Status des Servers "wodmProfile", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

   Das Symbol zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

   Das Symbol zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

   Das Symbol zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Knotenagent (nodeagent) unter Umständen nicht aktiv. Sie können den Knotenagenten (nodeagent) starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` ausführen.

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. wodmServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. wodmServer1
b. nodeagent

Um den Server "wodmProfile" zu stoppen, wählen Sie den Server aus und klicken Sie auf auf die entsprechende Option.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS-Administratorkennwort` ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

5. Überprüfen Sie, ob vom Anwendungsserver aus unter `http://Anwendungsserver-Host:9083/res` ein Zugriff auf die Rule Execution Server-Konsole möglich ist; dabei steht *Anwendungsserver-Host* für den Hostnamen des Anwendungsservers. Melden Sie sich mit der Benutzer-ID `resAdmin1` an.
6. Öffnen Sie in der Rule Execution Server-Konsole die Registerkarte "Diagnostics" (Diagnose) und klicken Sie auf **Run Diagnostics** (Diagnoseprogramm ausführen). Ein Bericht mit den Tests, die ausgeführt wurden, wird angezeigt. Klicken Sie auf **Expand All** (Alle einblenden), um die Details zu den einzelnen Tests anzuzeigen.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Business Rules (WebSphere Operational Decision Manager JRules Rule)"

Mit dem Test "Business Rules (WebSphere Operational Decision Manager JRules Rule)" wird der Zugriff auf die WebSphere Operational Decision Management JRules-Regelengine getestet; dazu wird die auf dem Rules Execution Server installierte Geschäftsregel `cardTransactionRuleApp` aufgerufen und die Ausgabe überprüft.

Ressourcen

Für den Test "Business Rules (WebSphere Operational Decision Manager JRules Rule)" wird die folgende Ressource verwendet:

- WebSphere Operational Decision Management JRules (auf dem Anwendungsserver).

Fehlerbestimmung

Schlägt der Test "Business Rules (WebSphere Operational Decision Manager JRules Rule)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Operational Decision Management-Konfigurationsprotokolle:
      - `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log`
2. Überprüfen Sie, ob die Kapazität des Dateisystems auf dem Anwendungsserver erreicht wurde (dies kann mit dem Befehl **`df -h`** festgestellt werden).
3. Überprüfen Sie, ob Rule Execution Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:
   a. Melden Sie sich auf dem Anwendungsserversystem als `ibmadmin` an.
   b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *`WAS-Administratorkennwort`* aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh`. Wird die Nachricht `ADMU0508I: The Application Server "nodeagent" is STARTED.` (Der Anwendungsserver "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server nodeagent open for e-business; process id is 26654` (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).
   a. Wird die Nachricht `ADMU0509I: The Application Server "wodmServer1" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "cpudServer1" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "wodmServer1" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1`. Wird die Nachricht `ADMU0508I: The Application Server "wodmServer1" is STARTED.` (Der Anwendungsserver "wodmServer1" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "wodmServer1" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server wodmServer1 open for e-business; process id is 26654` (Server "wodmServer1" ist für E-Business verfügbar; Prozess-ID ist 26654).

   Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

   Starten Sie die Server in der folgenden Reihenfolge:
   a. nodeagent
   b. wodmServer1

   Stoppen Sie die Server in der folgenden Reihenfolge:
   a. wodmServer1
   b. nodeagent

Der Server "wodmServer1" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password WAS-Administratorkennwort` ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS-Administratorkennwort` ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

4. Überprüfen Sie, ob Rule Execution Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung mithilfe der Administrationskonsole von WebSphere Application Server durch:
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://Anwendungsserver-Host:9060/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Anwendungsserver-Host* ist der Hostname für den Anwendungsserver.
   b. Überprüfen Sie den Status des Servers "wodmProfile", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

      Das Symbol zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

      Das Symbol zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

      Das Symbol zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Knotenagent (nodeagent) unter Umständen nicht aktiv. Sie können den Knotenagenten (nodeagent) starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` ausführen.

   Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

   Starten Sie die Server in der folgenden Reihenfolge:
   a. nodeagent
   b. wodmServer1

   Stoppen Sie die Server in der folgenden Reihenfolge:
   a. wodmServer1
   b. nodeagent

   Um den Server "wodmProfile" zu stoppen, wählen Sie den Server aus und klicken Sie auf auf die entsprechende Option.

   Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS-Administratorkennwort` ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.
5. Überprüfen Sie, ob vom Anwendungsserver aus unter `http://Anwendungsserver-Host:9083/res` ein Zugriff auf die Rule Execution Server-Konsole möglich ist; dabei steht *Anwendungsserver-Host* für den Hostnamen des Anwendungsservers. Melden Sie sich mit der Benutzer-ID `resAdmin1` an.
6. Öffnen Sie in der Rule Execution Server-Konsole die Registerkarte "Diagnostics" (Diagnose) und klicken Sie auf **Run Diagnostics** (Diagnoseprogramm ausführen). Ein Bericht mit den Tests, die ausgeführt wurden, wird angezeigt. Klicken Sie auf **Expand All** (Alle einblenden), um die Details zu den einzelnen Tests anzuzeigen.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Collaboration (Lotus Domino Console)"

Mit dem Test "Collaboration (Lotus Domino Console)" wird festgestellt, ob Domino Directory über die URL erreicht werden kann.

Ressourcen

Für den Test "Collaboration (Lotus Domino Console)" wird die folgende Ressource verwendet:

- Domino Server (auf dem Ereignisserver).

Fehlerbestimmung

Schlägt der Test "Collaboration (Lotus Domino Console)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Ereignisserver die folgenden Lotus Domino-Protokolle:
      - `/local/notesdata/console.out`
      - `/local/notesdata/log.nsf`
      - Alle Protokolle im Verzeichnis `/local/notesdata/IBM_TECHNICAL_SUPPORT/`
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Ereignisserversystem erreicht wurde (dies kann mit dem Befehl **`df -h`** festgestellt werden).
3. Überprüfen Sie, ob die Lotus Domino-Prozesskomponenten aktiv sind.
   a. Melden Sie sich an der Lotus Domino Directory-Konsole unter `http://`*`Ereignisserver-Host`*`:84/names.nsf` an; dabei ist *Ereignisserver-Host* der Hostname des Ereignisservers (melden Sie sich mit dem Benutzernamen und Kennwort des Domino-Administrators an).
   b. Ist kein Zugriff auf die Konsole möglich, führen Sie auf dem Ereignisserver den Befehl `ps -ef | grep notes` aus, um festzustellen, ob die Lotus Domino-Prozesse aktiv sind. Dabei handelt es sich um die folgenden Lotus Domino-Prozesse:
      - server
      - event
      - update
      - replica
      - router
      - adminp
      - calconn
      - sched
      - http
      - rnrmgr
      - staddin
4. Sind nur einige Prozesse aktiv, müssen Sie die aktiven Prozesse zunächst stoppen und anschließend alle Prozesse erneut starten.
   a. Melden Sie sich auf dem Ereignisserver als Benutzer `notes` an.
   b. Wechseln Sie in das Verzeichnis `/local/notesdata`.
   c. Führen Sie den Befehl `"nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &"` aus, um alle aktiven Lotus Domino-Prozesse zu stoppen.
   d. Überprüfen Sie mit dem Befehl `ps -ef | grep notes`, ob alle Prozesse gestoppt wurden.
   e. Sind einige Lotus Domino-Prozesse immer noch aktiv, müssen Sie sie mit dem Befehl **`kill -9`** *Prozess-ID* stoppen; dabei ist *Prozess-ID* die Prozess-ID des Lotus Domino-Prozesses.

5. Sind die Lotus Domino-Prozesse nicht (mehr) aktiv, starten Sie die Lotus Domino Server-Komponenten.
   a. Melden Sie sich auf dem Ereignisserver als Benutzer `notes` an.
   b. Wechseln Sie in das Verzeichnis `/local/notesdata`.
   c. Führen Sie den Befehl `"nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &"` aus, um alle Lotus Domino Server-Komponenten zu starten.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Collaboration (Lotus Sametime Console)"

Mit dem Test "Collaboration (Lotus Sametime Console)" wird festgestellt, ob die Sametime-Konsole über die URL erreicht werden kann.

Ressourcen

Für den Test "Collaboration (Lotus Sametime Console)" wird die folgende Ressource verwendet:

- Sametime-Server (auf dem Ereignisserver).

Fehlerbestimmung

Schlägt der Test "Collaboration (Lotus Sametime Console)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Erfassen Sie die die Konfigurations- und Protokolldateien für den Sametime Community-Server und überprüfen Sie diese Dateien.
   a. Melden Sie sich auf dem Ereignisserver als Benutzer *notes* an.
   b. Wechseln Sie in das Verzeichnis `/local/notesdata`.
   c. Führen Sie den Befehl `sh stdiagzip.sh` aus. Mit diesem Befehl werden alle relevanten Protokolldateien erfasst und in das Verzeichnis `/local/notesdata/` geschrieben.
   d. Überprüfen Sie die Protokolldateien im Verzeichnis `/local/notesdata/`.
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Ereignisserversystem erreicht wurde (dies kann mit dem Befehl **`df -h`** festgestellt werden).
3. Überprüfen Sie, ob die Sametime-Prozesskomponenten aktiv sind.
   a. Melden Sie sich auf der Sametime-Homepage unter `http://`*`Ereignisserver-Host`*`:84/stcenter.nsf` an; dabei ist *Ereignisserver-Host* der Hostname des Ereignisservers (melden Sie sich mit dem Benutzernamen und Kennwort des Domino-Administrators an).
   b. Klicken Sie auf der Sametime-Homepage auf **Administer the server** (Serververwaltung).
   c. Prüfen Sie auf der Serverübersichtsseite, ob alle Sametime-Services aktiv sind.
4. Sind nur einige Prozesse aktiv, müssen Sie die aktiven Prozesse zunächst stoppen und anschließend alle Prozesse erneut starten.
   a. Melden Sie sich auf dem Ereignisserver als Benutzer `notes` an.
   b. Wechseln Sie in das Verzeichnis `/local/notesdata`.
   c. Führen Sie den Befehl `"nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &"` aus, um alle aktiven Sametime-Prozesse zu stoppen.
   d. Überprüfen Sie mit dem Befehl `ps -ef | grep notes`, ob alle Prozesse gestoppt wurden.
   e. Sind einige Prozesse immer noch aktiv, müssen Sie sie mit dem Befehl **`kill -9`** *Prozess-ID* stoppen; dabei ist *Prozess-ID* die Prozess-ID des Lotus Domino-Prozesses.
5. Sind die Sametime-Prozesse nicht aktiv, starten Sie die Lotus Sametime-Serverkomponenten.
   a. Melden Sie sich auf dem Ereignisserver als Benutzer `notes` an.

b. Wechseln Sie in das Verzeichnis /local/notesdata.
c. Führen Sie den Befehl "nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &" aus, um alle Lotus Sametime-Serverkomponenten zu starten.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Collaboration (Lotus Sametime Proxy)"

Mit dem Test "Collaboration (Lotus Sametime Proxy)" wird festgestellt, ob die Lotus Sametime-Proxy-Webanwendung über die URL der Lotus Sametime-Proxy-Webanwendung erreicht werden kann.

Ressourcen

Für den Test "Collaboration (Lotus Sametime Proxy)" wird die folgende Ressource verwendet:

- Sametime-Proxy (auf dem Anwendungsserver).

Fehlerbestimmung

Schlägt der Test "Collaboration (Lotus Sametime Proxy)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Zugriffsproblem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
   b. Überprüfen Sie auf dem Anwendungsserver die folgenden Sametime-Proxy-Server-Protokolle:
      - /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log
      - /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Anwendungsserversystem erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
3. Überprüfen Sie, ob der Sametime-Proxy-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:
   a. Melden Sie sich auf dem Anwendungsserversystem als ibmadmin an.
   b. Führen Sie in einem Befehlsfenster den Befehl /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/serverStatus.sh -all -username waswebadmin -password *WAS-Administratorkennwort* aus; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped. (Der Anwendungsserver "nodeagent" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl /opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh. Wird die Nachricht ADMU0508I: The Application Server "nodeagent" is STARTED. (Der Anwendungsserver "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: ADMU3000I: Server nodeagent open for e-business; process id is 26654 (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).
   d. Wird die Nachricht ADMU0509I: The Application Server "STProxyServer1" cannot be reached. It appears to be stopped. (Der Anwendungsserver "STProxyServer1" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "STProxyServer1" mit dem Befehl /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/startServer.sh STProxyServer1.

Wird die Nachricht `ADMU0508I: The Application Server "STProxyServer1" is STARTED.` (Der Anwendungsserver "STProxyServer1" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "STProxyServer1" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server STProxyServer1 open for e-business; process id is 26654` (Server "STProxyServer1" für E-Business verfügbar; Prozess-ID ist 26654).

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. STProxyServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. STProxyServer1
b. nodeagent

Der Server "STProxyServer1" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopServer.sh STProxyServer1 -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

4. Überprüfen Sie, ob der Sametime-Proxy-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung über die Administrationskonsole von WebSphere Application Server durch:
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://`*`Anwendungsserver-Host`*`:9060/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Anwendungsserver-Host* ist der Hostname für den Anwendungsserver.
   b. Überprüfen Sie den Status des Servers "STProxyServer1", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

      Das Symbol  zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

      Das Symbol  zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

      Das Symbol  zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Knotenagent (nodeagent) unter Umständen nicht aktiv. Sie können den Knotenagenten starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh` ausführen.

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. STProxyServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. STProxyServer1
b. nodeagent

Um den Server "STProxyServer1" zu stoppen, wählen Sie den Server aus und klicken Sie auf die entsprechende Option.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

5. Überprüfen Sie, ob der Zugriff auf die Sametime-Proxy-Konsole vom WebSphere Portal-System auf dem Anwendungsserver aus über die URL `http://`*`Anwendungsserver-Host`*`:9085/stwebclient/popup.jsp` möglich ist; dabei ist *Anwendungsserver-Host* der Hostname für den Anwendungsserver.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Database (DB2)"

Mit dem Test "Database (DB2)" wird festgestellt, ob ein Zugriff auf die JDBC-Verbindung zwischen der Webanwendung und dem Datenserver möglich ist. Dazu wird eine JDBC-Verbindung (Typ 4) hergestellt und eine dynamische SQL-Abfrage ausgegeben, mit der die Anzahl der in der Datenbank vorhandenen Tabellen festgestellt werden soll.

Ressourcen

Für den Test "Database (DB2)" werden die folgenden Ressourcen verwendet:

- Die Definition `UddiDataSource`; sie enthält die Verbindung für die UDDIDB-Datenbank (auf dem Anwendungsserver).
- UDDIDB-Datenbank (Instanz "db2inst4" auf dem Datenserver).

Fehlerbestimmung

Wenn bei Ausführung des Tests "Database (DB2)" kein Zugriff auf den Datenserver möglich ist, gehen Sie wie im Folgenden beschrieben vor, um das Zugriffsproblem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem Anwendungsserver, auf dem der Test gestartet wurde, und dem Datenserver, auf dem sich die Datenbank befindet, eine Netzverbindung besteht. Dazu können vom Anwendungsserver aus **ping**-Befehle mit dem kurzen und dem vollständig qualifizierten Hostnamen des Datenservers gesendet werden. Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Datenserversystem erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
4. Überprüfen Sie, ob die vom Datenserver verwendeten Datenbanken gestartet wurden.
   a. Führen Sie in einem Befehlsfenster auf dem Datenserver als Benutzer "db2inst4" den folgenden Befehl aus:

      ```
      ps -ef | grep db2 | grep db2inst4
      ```

      DB2-Prozesse, einschließlich der folgenden, sollten als Instanzbenutzer "db2inst4" ausgeführt werden:

      db2sysc
      db2vend

db2acd

5. Sind die DB2-Prozesse nicht aktiv, starten Sie sie, indem Sie als Benutzer "db2inst4" in einem Befehlsfenster `db2start` ausführen:
6. Überprüfen Sie die DB2-Protokolle auf Fehler in Zusammenhang mit der Datenbankinstanz, die für diesen Test verwendet wird. Diese Protokolle befinden sich im Verzeichnis `/datahome/db2inst4/sqllib/db2dump` auf dem Datenserver.
7. Überprüfen Sie das Protokoll `db2diag.log` auf Fehlernachrichten, die beim Start der für diesen Test verwendeten Datenbank ausgegeben wurden.
8. Überprüfen Sie die Verbindung zu den DataSource-Web-Container-Ressourcen mithilfe der Verwaltungskonsole von WebSphere Application Server.
   a. Rufen Sie auf dem Anwendungsserver unter `https://`*`Anwendungsserver-Host`*`:9043/ibm/console` die Verwaltungskonsole von WebSphere Application Server auf; dabei ist *Anwendungsserver-Host* der Hostname des Anwendungsservers.
   b. Klicken Sie auf **Resources** > **JDBC** > **Data sources** (Ressourcen > JDBC > Datenquellen).
   c. Überprüfen Sie die Datenquelle "UddiDataSource", indem Sie auf **Test Connection** (Verbindung testen) klicken, um die Verbindung zur Datenquelle zu prüfen.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Database (DB2 Instance - *Instanz*)"

Mit dem Test "Database (DB2 Instance - *Instanz*)" wird der Status des DB2-Managers der DB2-Instanz auf dem Datenserver durch Ausführung des Scripts **`db2status`** geprüft.

Ressourcen

Für den Test "Database (DB2 Instance - *Instanz*)" wird die folgende Ressource verwendet:

- Die DB2-*Instanz* (auf dem Datenserver)

Fehlerbestimmung

Schlägt der Test "Database (DB2 Instance - *Instanz*)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Zugriffsproblem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem Anwendungsserver, auf dem der Test gestartet wurde, und dem Datenserver, auf dem sich die Datenbank befindet, eine Netzverbindung besteht. Dazu können vom Anwendungsserver aus **`ping`**-Befehle mit dem kurzen und dem vollständig qualifizierten Hostnamen des Datenservers gesendet werden. Aus dem Ergebnis dieser **`ping`**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Überprüfen Sie, ob die Kapazität des Dateisystems auf dem Datenserversystem erreicht wurde (dies kann mit dem Befehl **`df -h`** festgestellt werden).
4. Überprüfen Sie, ob die vom Datenserver verwendeten Datenbanken gestartet wurden.
   a. Führen Sie in einem Befehlsfenster auf dem Datenserver als Benutzer *Instanz* den folgenden Befehl aus (dabei ist *Instanz* der Name der im Testnamen angegebenen DB2-Instanz):

      ```
      db2 get snapshot for dbm | grep status
      ```

Wurde der Datenbankmanager für die *Instanz* gestartet, wird die folgende Nachricht angezeigt: `Database manager status = Active` (Status des Datenbankmanagers = Aktiv).

5. Sind die DB2-Prozesse nicht aktiv, starten Sie sie, indem Sie im Befehlsfenster den Befehl **su -** *Instanz* ausführen (wenn sie als Benutzer `root` aktiv sind). Andernfalls müssen Sie den Datenbankmanager durch Ausführung von **db2start** starten.
6. Überprüfen Sie die DB2-Protokolle auf Fehler in Zusammenhang mit der Datenbankinstanz, die für diesen Test verwendet wird. Diese Protokolle befinden sich im Verzeichnis `/datahome/`*`Instanz`*`/sqllib/db2dump` auf dem Datenserver.
7. Überprüfen Sie das Protokoll `db2diag.log` auf Fehlernachrichten, die beim Start der für diesen Test verwendeten Datenbank ausgegeben wurden.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Directory (UDDI V3 and UDDI V3 HTTPS)"

Mit dem Test "Directory (UDDI V3 and UDDI V3 HTTPS)" wird festgestellt, ob der Zugriff auf die WebSphere-UDDI-Registry über die HTTP- und HTTPS-URL der WebSphere-UDDI-Registry möglich ist.

Ressourcen

Für den Test "Directory (UDDI V3 and UDDI V3 HTTPS)" wird die folgende Ressource verwendet:

- WebSphere Application Server (auf dem Anwendungsserver).

Fehlerbestimmung

Schlägt der Test "Directory (UDDI V3 and UDDI V3 HTTPS)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Zugriffsproblem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere-UDDI-Registry-Konfigurationsprotokolle:
      - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log`
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Anwendungsserversystem erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
3. Überprüfen Sie, ob der Server "cpudServer1" gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:
   a. Melden Sie sich auf dem Anwendungsserversystem als `ibmadmin` an.
   b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *`WAS-Administratorkennwort`* aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh`. Wird die Nachricht `ADMU0508I: The Application Server "nodeagent" is STARTED.` (Der Anwendungs-

server "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server nodeagent open for e-business; process id is 26654` (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).

a. Wird die Nachricht `ADMU0509I: The Application Server "cpudServer1" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "cpudServer1" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "cpudServer1" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1`. Wird die Nachricht `ADMU0508I: The Application Server "cpudServer1" is STARTED.` (Der Anwendungsserver "cpudServer1" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "cpudServer1" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server cpudServer1 open for e-business; process id is 26654` (Server "cpudServer1" für E-Business verfügbar, Prozess-ID ist 26654.)

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. cpudServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. cpudServer1
b. nodeagent

Der Server "cpudServer1" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

4. Überprüfen Sie, ob der Server "cpudServer1" gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung mithilfe der Administrationskonsole von WebSphere Application Server durch:
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://`*`Anwendungsserver-Host`*`:9060/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Anwendungsserver-Host* ist der Hostname für den Anwendungsserver.
   b. Überprüfen Sie den Status des Servers "cpudServer1", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

      Das Symbol zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

      Das Symbol zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

      Das Symbol zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Knotenagent (nodeagent) unter Umständen nicht aktiv. Sie können den Knotenagenten starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh` ausführen.

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. cpudServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. cpudServer1
b. nodeagent

Um den Server "cpudServer" zu stoppen, wählen Sie den Server aus und klicken Sie auf die entsprechende Option.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

5. Überprüfen Sie, ob der Zugriff auf die Benutzerkonsole der WebSphere-UDDI-Registry vom WebSphere Portal-System auf dem Anwendungsserver aus über die URL `http://`*`Anwendungsserver-Host`*`:9080/uddigui/` möglich ist; dabei ist *Anwendungsserver-Host* der Hostname für den Anwendungsserver.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Internal Diagnostic (Echo REST remoted)"

Mit dem Test "Internal Diagnostic (Echo REST remoted)" wird der Zugriff auf den Remote-Responder über die URL geprüft. Hierbei handelt es sich um eine Diagnose der Systemprüfung, bei der die Verbindungen zwischen Systemprüfungsmodulen überprüft werden.

Ressourcen

Für den Test "Internal Diagnostic (Echo REST remoted)" wird die folgende Ressource verwendet:

- WebSphere Application Server (auf dem Anwendungsserver).

Fehlerbestimmung

Schlägt der Test "Internal Diagnostic (Echo REST remoted)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere-UDDI-Registry-Konfigurationsprotokolle:
      - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log`
2. Überprüfen Sie, ob die Kapazität des Dateisystems auf dem Anwendungsserver erreicht wurde (dies kann mit dem Befehl **`df -h`** festgestellt werden).
3. Überprüfen Sie, ob der Server "cpudServer1" gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:
   a. Melden Sie sich auf dem Anwendungsserversystem als `ibmadmin` an.

b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS-Administratorkennwort` aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.

c. Wird die Nachricht `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh`. Wird die Nachricht `ADMU0508I: The Application Server "nodeagent" is STARTED.` (Der Anwendungsserver "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server nodeagent open for e-business; process id is 26654` (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).

a. Wird die Nachricht `ADMU0509I: The Application Server "cpudServer1" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "cpudServer1" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "cpudServer1" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1`. Wird die Nachricht `ADMU0508I: The Application Server "cpudServer1" is STARTED.` (Der Anwendungsserver "cpudServer1" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "cpudServer1" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server cpudServer1 open for e-business; process id is 26654` (Server "cpudServer1" für E-Business verfügbar, Prozess-ID ist 26654.)

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent

b. cpudServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. cpudServer1

b. nodeagent

Der Server "cpudServer1" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS-Administratorkennwort` ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS-Administratorkennwort` ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

4. Überprüfen Sie, ob der Server "cpudServer1" gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung mithilfe der Administrationskonsole von WebSphere Application Server durch:

   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://Anwendungsserver-Host:9060/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Anwendungsserver-Host* ist der Hostname für den Anwendungsserver.

   b. Überprüfen Sie den Status des Servers "cpudServer1", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

      Das Symbol zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

Das Symbol  zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

Das Symbol  zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Knotenagent (nodeagent) unter Umständen nicht aktiv. Sie können den Knotenagenten starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh` ausführen.

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. cpudServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. cpudServer1
b. nodeagent

Um den Server "cpudServer" zu stoppen, wählen Sie den Server aus und klicken Sie auf die entsprechende Option.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

5. Überprüfen Sie, ob ein Zugriff auf die WebSphere-UDDI-Benutzerkonsole möglich ist.
   a. Rufen Sie auf dem Anwendungsserver `https://`*`Anwendungsserver-Host`*`:9080/uddigui/` auf. Dabei steht *Anwendungsserver-Host* für den Hostnamen des Anwendungsservers.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Messaging (WebSphere Message Broker Publish/Subscribe topic)"

Mit dem Test "Messaging (WebSphere Message Broker Publish/Subscribe topic)" werden die Publish-/Subscribe-Funktionen von WebSphere Message Broker überprüft. Dabei wird zu dem Thema mit dem in den Eigenschaften als `jms/IopCatWmbPub` aufgeführten JNDI-Namen eine Nachricht veröffentlicht. WebSphere Message Broker erhält diese Nachricht und veröffentlicht eine Antwortnachricht zum Thema `IOP.CAT.PUB`. Wird die Antwortnachricht erhalten, war der Test erfolgreich. Tritt ein Fehler auf oder wird die Antwortnachricht nicht innerhalb des in der Eigenschaftendatei definierten Zeitlimitintervalls empfangen, ist der Test fehlgeschlagen.

Ressourcen

Für den Test "Messaging (WebSphere Message Broker Publish/Subscribe topic)" werden die folgenden Ressourcen verwendet:

- WebSphere Portal Server (auf dem Anwendungsserver).
- WebSphere Message Queue (auf dem Ereignisserver).
- WebSphere Message Broker (auf dem Ereignisserver).

Fehlerbestimmung

Schlägt der Test "Messaging (WebSphere Message Broker Publish/Subscribe topic)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem Anwendungsserver und dem Ereignisserver eine Netzverbindung besteht. Dazu können **ping**-Befehle mit dem kurzen und dem vollständig qualifizierten Hostnamen von den einzelnen bzw. an die einzelnen Server gesendet werden. Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Ereignisserver und dem Anwendungsserver erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
4. Überprüfen Sie, ob der WebSphere Message Queue-Warteschlangenmanager und der WebSphere Message Broker-Broker aktiv sind.
   a. Melden Sie sich auf dem Ereignisserver als WebSphere Message Queue-Administrator an. Beispiel: `mqm`.
   b. Führen Sie in einem Befehlsfenster den Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq** aus. Es wird eine Nachricht ähnlich der folgenden angezeigt:
      ```
      QMNAME(IOC.MB.QM) STATUS(Running)
      ```
   c. Wurde ein anderer Status als `Running` zurückgegeben, starten Sie den WebSphere Message Queue-Warteschlangenmanager mit dem Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
   d. Melden Sie sich auf dem Ereignisserver als WebSphere Message Broker-Administrator an. Beispiel: `mqm`.
   e. Führen Sie in einem Befehlsfenster den Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist** aus. Es wird eine Nachricht ähnlich der folgenden angezeigt:
      ```
      BIP1284I: Broker 'IOC_BROKER' on queue manager 'IOC.MB.QM' is running.
      ```
      (Broker 'IOC_BROKER' in WS-Manager 'IOC.MB.QM' ist aktiv.)
   f. Wurde ein anderer Status als `Running` (Aktiv) zurückgegeben, starten Sie den WebSphere Message Broker-Broker mit dem Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsistart IOC_BROKER**.
5. Überprüfen Sie die Protokolle auf Fehler. Die Protokolle befinden sich im Verzeichnis `/var/log/messages` auf dem Ereignisserver. Suchen Sie nach Nachrichten, denen "BIP" vorangestellt ist. Suchen Sie außerdem nach Warteschlangennamen und Zeitmarken für die Testausführung.
6. Sind der Broker oder die Warteschlangenmanager nicht aktiv, können sie auch gestartet werden, indem der Ereignisserver gestartet wird und die Startscripts für das System ausgeführt werden.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Messaging (WebSphere Message Queue Publish/Subscribe topic)"

Mit dem Test "Messaging (WebSphere Message Queue Publish/Subscribe topic)" werden die Publish-/Subscribe-Funktionen von WebSphere Message Queue überprüft. Bei diesem Test wird ein in den Eigenschaften angegebenes Thema erstellt. Anschließend wird vom Test eine Nachricht zu diesem Thema erstellt, die vom Test sofort gelesen wird. Kann die Nachricht gelesen werden, war der Test erfolgreich. Tritt ein Fehler auf oder kann die Nachricht nicht innerhalb von 15 Sekunden (15.000 Millisekunden) gelesen werden, ist der Test fehlgeschlagen.

Ressourcen

Für den Test "Messaging (WebSphere Message Queue Publish/Subscribe topic)" werden die folgenden Ressourcen verwendet:

- WebSphere Portal Server (auf dem Anwendungsserver).
- WebSphere Message Queue (auf dem Ereignisserver).

Fehlerbestimmung

Schlägt der Test "Messaging (WebSphere Message Queue Publish/Subscribe topic)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem Anwendungsserver und dem Ereignisserver eine Netzverbindung besteht. Dazu können **ping**-Befehle mit dem kurzen und dem vollständig qualifizierten Hostnamen von den einzelnen bzw. an die einzelnen Server gesendet werden. Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Überprüfen Sie, ob die Kapazität der Dateisysteme auf den Servern erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
4. Überprüfen Sie, ob der WebSphere Message Queue-Warteschlangenmanager aktiv ist.
   a. Melden Sie sich auf dem Ereignisserver als WebSphere Message Queue-Administrator an. Beispiel: `mqm`.
   b. Führen Sie in einem Befehlsfenster den Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq** aus. Es wird eine Nachricht ähnlich der folgenden angezeigt:
      ```
      QMNAME(IOC.MB.QM) STATUS(Running)
      ```
   c. Wurde ein anderer Status als `Running` zurückgegeben, starten Sie den WebSphere Message Queue-Warteschlangenmanager mit dem Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
5. Überprüfen Sie die Protokolle auf Fehler. Die Protokolle befinden sich im Verzeichnis `/var/log/messages` auf dem Ereignisserver. Suchen Sie nach Nachrichten, denen "BIP" vorangestellt ist. Suchen Sie außerdem nach Warteschlangennamen und Zeitmarken für die Testausführung.
6. Ist der Warteschlangenmanager nicht aktiv, kann er auch gestartet werden, indem der Ereignisserver gestartet wird und die Startscripts für das System ausgeführt werden.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Messaging (WebSphere Message Broker/Queue install check)"

Mit dem Test "Messaging (WebSphere Message Broker/Queue install check)" wird festgestellt, ob ein Zugriff auf WebSphere Message Queue und Message Broker möglich ist. Dazu wird auf dem System, auf dem WebSphere Message Broker aktiv ist, der WebSphere Message Broker-Befehl **mqsilist** ausgeführt.

Ressourcen

Für den Test "Messaging (WebSphere Message Broker/Queue install check)" werden die folgenden Ressourcen verwendet:

- WebSphere Portal Server (auf dem Anwendungsserver).
- WebSphere Message Queue und Message Broker (auf dem Ereignisserver).

Fehlerbestimmung

Schlägt der Test "Messaging (WebSphere Message Broker/Queue install check)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem WebSphere Portal-System (auf dem Anwendungsserver) und dem WebSphere Message Broker-System (auf dem Ereignisserver) eine Netzverbindung besteht. Dazu können vom Anwendungsserver aus **ping**-Befehle mit dem kurzen und dem vollständigen Hostnamen des Ereignisservers gesendet werden (und umgekehrt). Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Überprüfen Sie, ob die Kapazität der Dateisysteme auf den Anwendungsserver- und Ereignisserversystemen erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
4. Überprüfen Sie, ob der WebSphere Message Queue-Warteschlangenmanager und der WebSphere Message Broker-Broker aktiv sind.
   a. Melden Sie sich auf dem Ereignisserver als WebSphere Message Queue-Administrator an. Beispiel: `mqm`.
   b. Führen Sie in einem Befehlsfenster den Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq** aus. Es wird eine Nachricht ähnlich der folgenden angezeigt:
      ```
      QMNAME(IOC.MB.QM) STATUS(Running)
      ```
   c. Wurde ein anderer Status als `Running` zurückgegeben, starten Sie den WebSphere Message Queue-Warteschlangenmanager mit dem Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
   d. Melden Sie sich auf dem Ereignisserver als WebSphere Message Broker-Administrator an. Beispiel: `mqm`.
   e. Führen Sie in einem Befehlsfenster den Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist** aus. Es wird eine Nachricht ähnlich der folgenden angezeigt:
      ```
      BIP1284I: Broker 'IOC_BROKER' on queue manager 'IOC.MB.QM' is running.
      ```
      (Broker 'IOC_BROKER' in WS-Manager 'IOC.MB.QM' ist aktiv.)
   f. Wurde ein anderer Status als `Running` (Aktiv) zurückgegeben, starten Sie den WebSphere Message Broker-Broker mit dem Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsistart IOC_BROKER**.
5. Überprüfen Sie die Protokolle auf Fehler. Die Protokolle befinden sich im Verzeichnis `/var/log/messages` auf dem Ereignisserver. Suchen Sie nach Nachrichten, denen "BIP" vorangestellt ist. Suchen Sie außerdem nach Warteschlangennamen und Zeitmarken für die Testausführung.
6. Sind der Broker oder die Warteschlangenmanager nicht aktiv, können sie auch gestartet werden, indem der Ereignisserver gestartet wird und die Startscripts für das System ausgeführt werden.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Messaging (WebSphere Message Broker/Queue queue)"

Mit dem Test "Messaging (WebSphere Message Broker/Queue queue)" wird WebSphere Message Queue geprüft, indem eine Nachricht in eine Warteschlange gestellt wird.

Ressourcen

Für den Test "Messaging (WebSphere Message Broker/Queue queue)" werden die folgenden Ressourcen verwendet:

- WebSphere Portal Server (auf dem Anwendungsserver).
- WebSphere Message Queue (auf dem Ereignisserver).
- WebSphere Message Broker (auf dem Ereignisserver).

Fehlerbestimmung

Schlägt der Test "Messaging (WebSphere Message Broker/Queue queue)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem Anwendungsserver und dem Ereignisserver eine Netzverbindung besteht. Dazu können **ping**-Befehle mit dem kurzen und dem vollständig qualifizierten Hostnamen von den einzelnen bzw. an die einzelnen Server gesendet werden. Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Überprüfen Sie, ob die Kapazität der Dateisysteme auf den Anwendungsserver- und Ereignisserversystemen erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
4. Überprüfen Sie, ob der WebSphere Message Queue-Warteschlangenmanager und der WebSphere Message Broker-Broker aktiv sind.
   a. Melden Sie sich auf dem Ereignisserver als WebSphere Message Queue-Administrator an. Beispiel: `mqm`.
   b. Führen Sie in einem Befehlsfenster den Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq** aus. Es wird eine Nachricht ähnlich der folgenden angezeigt:
      ```
      QMNAME(IOC.MB.QM) STATUS(Running)
      ```
   c. Wurde ein anderer Status als `Running` zurückgegeben, starten Sie den WebSphere Message Queue-Warteschlangenmanager mit dem Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**.
   d. Melden Sie sich auf dem Ereignisserver als WebSphere Message Broker-Administrator an. Beispiel: `mqm`.
   e. Führen Sie in einem Befehlsfenster den Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist** aus. Es wird eine Nachricht ähnlich der folgenden angezeigt:
      ```
      BIP1284I: Broker 'IOC_BROKER' on queue manager 'IOC.MB.QM' is running.
      ```
      (Broker 'IOC_BROKER' in WS-Manager 'IOC.MB.QM' ist aktiv.)
   f. Wurde ein anderer Status als `Running` (Aktiv) zurückgegeben, starten Sie den WebSphere Message Broker-Broker mit dem Befehl **source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsistart IOC_BROKER**.
5. Überprüfen Sie die Protokolle auf Fehler. Die Protokolle befinden sich im Verzeichnis `/var/log/messages` auf dem Ereignisserver. Suchen Sie nach Nachrichten, denen "BIP" vorangestellt ist. Suchen Sie außerdem nach Warteschlangennamen und Zeitmarken für die Testausführung.
6. Sind der Broker oder die Warteschlangenmanager nicht aktiv, können sie auch gestartet werden, indem der Ereignisserver gestartet wird und die Startscripts für das System ausgeführt werden.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Monitoring (Netcool Impact Console)"

Mit dem Test "Monitoring (Netcool Impact Console)" wird festgestellt, ob die Netcool/Impact-Konsole aktiv ist und über die Netcool/Impact-Konsolen-URL erreicht werden kann.

Ressourcen

Für den Test "Monitoring (Netcool Impact Console)" wird die folgende Ressource verwendet:

- Netcool/Impact-Server (auf dem Ereignisserver)

Fehlerbestimmung

Schlägt der Test "Monitoring (Netcool Impact Console)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Ereignisserver die folgenden Netcool Impact-Protokolle:
      - `/opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log`
      - `/opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log`
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Ereignisserversystem erreicht wurde (dies kann mit dem Befehl **`df -h`** festgestellt werden).
3. Überprüfen Sie, ob der Server "server1" gestartet wurde.
   a. Melden Sie sich auf dem Ereignisserversystem als `wasadmin` an.
   b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/serverStatus.sh -all -username wasadmin -password` *`WAS-Administratorkennwort`* aus; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht `ADMU0509I: The Application Server "server1" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "server1" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie mit dem Befehl `/opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/startServer.sh server1` den Server "server1"; damit wird auch der Netcool/Impact-Konsolenserver gestartet. Wird die Nachricht `ADMU0508I: The Application Server "server1" is STARTED` (Der Anwendungsswerver "server1" wurde gestartet.) angezeigt, kann dieser Schritt übersprungen werden. Wenn Sie den Server "server1" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server server1 open for e-business; process id is 26654` (Server "server1" ist für E-Business verfügbar; Prozess-ID ist 26654).

   Der Server "server1" wird gestoppt, indem in einem Befehlsfenster auf dem Ereignisserver der Befehl `/opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/stopServer.sh server1 -username wasadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.
4. Überprüfen Sie, ob vom Ereignisserver aus unter `http://`*`Ereignisserver-Host`*`:9080/nci` ein Zugriff auf die Netcool/Impact-Konsole möglich ist; dabei ist *Ereignisserver-Host* der Hostname des Ereignisservers.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Monitoring (Netcool Omnibus)"

Mit dem Test "Monitoring (Netcool Omnibus)" wird festgestellt, ob Netcool/OMNIbus verfügbar ist. Dazu wird der Befehl **nco_pa_status -server NCO_PA** ausgeführt.

Ressourcen

Für den Test "Monitoring (Netcool Omnibus)" wird die folgende Ressource verwendet:

- Netcool/OMNIbus-Server (auf dem Ereignisserver)

Fehlerbestimmung

Schlägt der Test "Monitoring (Netcool Omnibus)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem Anwendungsserver und dem Ereignisserver eine Netzverbindung besteht. Dazu können vom Anwendungsserver aus **ping**-Befehle mit dem kurzen und dem vollständig qualifizierten Hostnamen des Ereignisservers gesendet werden. Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie, ob die Serverdienste und der Agent für die Prozesssteuerung aktiv sind.
   a. Führen Sie als Linux-Benutzer *netcool* in einem Befehlsfenster auf dem Ereignisserver den Befehl **$NCHOME/omnibus/bin/nco_pa_status -server NCO_PA** aus.
   b. Werden die Services nicht gestartet bzw. sind sie nicht aktiv, starten Sie den Server, indem Sie auf dem Ereignisserver als ein Linux-Benutzer *root* den Befehl **/etc/init.d/nco start** ausführen.
   c. Ist der Prozessagent nicht aktiv, starten Sie ihn, indem Sie auf dem Ereignisserver als Linux-Benutzer *netcool* den Befehl **$NCHOME/omnibus/bin/nco_pad** ausführen.
3. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Ereignisserver in den folgenden Verzeichnissen alle Protokolle, die mit "NCO" beginnen:
      - `/opt/IBM/netcool/log`
      - `/opt/IBM/netcool/omnibus/log`
4. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Ereignisserversystem erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
5. Überprüfen Sie, ob vom Anwendungsserver aus unter `http://`*Ereignisserver-Host*`:9060/ibm/console` ein Zugriff auf das Netcool/OMNIbus-Portlet möglich ist; dabei ist *Ereignisserver-Host* der Hostname des Ereignisservers.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Monitoring (Tivoli Composite Application Manager Agents - *Server*)"

Mit dem Test "Monitoring (Tivoli Composite Application Manager Agents - *Server*)" wird durch Ausführung des Befehls **cinfo** festgestellt, ob die Tivoli Composite Application Manager-Agenten aktiv sind.

Ressourcen

Für den Test "Monitoring (Tivoli Composite Application Manager Agents - *Server*)" werden die folgenden Ressourcen verwendet:

- Tivoli Composite Application Manager
  - Tivoli Composite Application Manager-Agenten (auf dem Anwendungsserver)
  - Tivoli Composite Application Manager-Agenten (auf dem Ereignisserver)
  - Tivoli Composite Application Manager-Agenten (auf dem Datenserver)
  - Tivoli Composite Application Manager-Agenten (auf dem Verwaltungsserver)

Fehlerbestimmung

Schlägt der Test "Monitoring (Tivoli Composite Application Manager Agents - *Server*)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem Anwendungsserver, dem Verwaltungsserver, dem Ereignisserver und dem Datenserver eine Netzverbindung besteht. Dazu können vom Anwendungsserver aus **ping**-Befehle mit dem kurzen und dem vollständig qualifizierten Hostnamen des Verwaltungsservers, des Ereignisservers und des Datenservers gesendet werden. Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Anwendungsserver, dem Verwaltungsserver, dem Ereignisserver und dem Datenserver erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
4. Führen Sie diesen Schritt auf dem Anwendungsserver, dem Verwaltungsserver, dem Ereignisserver und dem Datenserver aus, um festzustellen, ob die Tivoli Monitoring-Komponenten aktiv sind.
   a. Melden Sie sich auf dem Server als `root` an einer Terminalsitzung an.
   b. Führen Sie den Befehl **/opt/IBM/ITM/bin/cinfo -r** aus. Das Ergebnis, das angezeigt wird, entspricht ungefähr dem hier dargestellten Text. Die Agenten variieren von Server zu Server. Die Agenten sollten den Status "running" (Aktiv) haben.

```
********** Sun May 13 02:13:26 EDT 2012 *****************
User: root Groups: root bin daemon sys adm disk wheel idsldap tdsproxy ivmgr tivoli
Host name : baapp2 Installer Lvl:06.22.01.00
CandleHome: /opt/IBM/ITM
***********************************************************
Host    Prod    PID    Owner    Start    ID     ..Status
baapp2  lz      31042  root     May09    None   ...running
baapp2  ht      18755  root     May09    None   ...running
baapp2  yn      4190   root     02:11    None   ...running
```

   c. Starten Sie alle Tivoli Composite Application Manager-Agenten, die nicht aktiv sind.
      1) Melden Sie sich auf dem Server als `root` an einer Terminalsitzung an.
      2) Führen Sie den Befehl **/opt/IBM/ITM/bin/itmcmd agent start** *Produktcode* aus; dabei ist *Produktcode* die PID für einen Agenten, die im Ergebnis des Befehls **/opt/IBM/ITM/bin/cinfo -o** enthalten ist.
5. Überprüfen Sie die Protokolldateien auf Ausnahmebedingungen.
   a. Überprüfen Sie auf dem Verwaltungsserver die folgenden Tivoli Enterprise Monitoring Server- und Tivoli Enterprise Portal Server-Protokolle:
      - Tivoli Enterprise Monitoring Server: `/opt/IBM/ITM/logs/*_PRODUKTCODE_{nnnnnnn}.log`
      - Tivoli Enterprise Portal Server: `/opt/IBM/ITM/logs/*_PRODUKTCODE_{nnnnnnn}.log`

      Dabei steht *Produktcode* für die vom Befehl **/opt/IBM/ITM/bin/cinfo -o** zurückgegebene PID.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Monitoring (Tivoli Enterprise Monitoring Server)"

Mit dem Test "Monitoring (Tivoli Enterprise Monitoring Server)" wird festgestellt, ob Tivoli Enterprise Monitoring Server auf dem Verwaltungsserver verfügbar ist. Dazu wird an die Tivoli Monitoring-Web-Services (SOAP-Server) eine Statusabfrage gesendet. Diese Abfrage enthält eine ungültige Benutzer-ID und ein ungültiges Kennwort für das System. In der Antwort sollte darauf hingewiesen werden, dass eine ungültige Benutzer-ID bzw. ein ungültiges Kennwort verwendet wurde. Diese Fehlernachricht weist darauf hin, dass Tivoli Enterprise Monitoring Server ordnungsgemäß arbeitet.

Ressourcen

Für den Test "Monitoring (Tivoli Enterprise Monitoring Server)" werden die folgenden Ressourcen verwendet:

- Tivoli Enterprise Monitoring-System (auf dem Verwaltungsserver)
  - Tivoli Monitoring-Web-Services (SOAP-Server)
  - Tivoli Enterprise-Portalserver
  - DB2-Datenbank für den Tivoli Enterprise-Portalserver

Fehlerbestimmung

Schlägt der Test "Monitoring (Tivoli Enterprise Monitoring Server)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob zwischen dem Anwendungsserver und dem Verwaltungsserver eine Netzverbindung besteht. Dazu können vom Anwendungsserver aus **ping**-Befehle mit dem kurzen und dem vollständig qualifizierten Hostnamen des Verwaltungsservers gesendet werden. Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wurde.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Verwaltungsserver die folgenden Verwaltungsserver-protokolle:
      - Tivoli Event Monitoring Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_ms_{nnnnnnn}.log`
      - Tivoli Event Portal Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_cq_{nnnnnnn}.log`
      - Embedded WebSphere Application Server-Protokolle:
        - Fehlerprotokoll: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log`
        - Ausgabeprotokoll: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log`
        - Startprotokoll: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/startServer.log`
3. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Verwaltungsserver erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
4. Überprüfen Sie, ob die Tivoli Monitoring-Komponenten auf dem Verwaltungsserver aktiv sind.
   a. Melden Sie sich auf dem Verwaltungsserver als `root` an einer Terminalsitzung an.
   b. Führen Sie den Befehl **/opt/IBM/ITM/bin/cinfo -r** aus.
5. Überprüfen Sie, ob die Tivoli-Komponentendatenbanken aktiv sind.

a. Melden Sie sich auf dem Verwaltungsserver als db2inst1 an einer Terminalsitzung an.
b. Führen Sie den Befehl **ps -ef | grep db2inst1** aus.
c. Überprüfen Sie, ob die DB2-Prozesse aktiv sind (dabei handelt es sich um "db2sysc", "db2vend" und "db2acd").
d. Sind die DB2-Prozesse nicht aktiv, führen Sie den Befehl **$> db2start** aus.
e. Überprüfen Sie die DB2-Protokolle auf dem Datenserver auf Fehler in Zusammenhang mit dem Start einer der von den Tivoli-Komponenten verwendeten Datenbanken. Diese Protokolldateien sind auf dem Datenserver im Verzeichnis /datahome/db2inst1/sqllib/db2dump enthalten.

6. Überprüfen Sie anhand des Ergebnisses, ob Tivoli Enterprise Monitoring Server aktiv ist, indem Sie nach einem Eintrag für ms suchen. Ist dieser Eintrag nicht enthalten, ist Tivoli Enterprise Monitoring Server nicht aktiv.
7. Ist Tivoli Enterprise Monitoring Server nicht aktiv, starten Sie den Server.
   a. Melden Sie sich auf dem Verwaltungsserver als root an einer Terminalsitzung an.
   b. Führen Sie den Befehl **/opt/IBM/ITM/bin/itmcmd server start HUB_MWOS** aus.
8. Überprüfen Sie anhand des Ergebnisses von Schritt 4 auf Seite 257, ob der Tivoli Enterprise-Portalserver aktiv ist, indem Sie nach einem Eintrag für cq suchen. Ist dieser Eintrag nicht enthalten, ist der Tivoli Enterprise-Portalserver nicht aktiv.
9. Ist der Tivoli Enterprise-Portalserver nicht aktiv, starten Sie den Server.
   a. Melden Sie sich auf dem Verwaltungsserver als root an einer Terminalsitzung an.
   b. Führen Sie den Befehl **/opt/IBM/ITM/bin/itmcmd agent start cq** aus.
10. Überprüfen Sie anhand des Ergebnisses von Schritt 4 auf Seite 257, ob weitere gültige Unterkomponenten aktiv sind.

Tabelle 79. Tivoli Monitoring-Komponenten

Komponente	Beschreibung
kf	Eclipse Help Server
cq	Tivoli Enterprise-Portalserver
lz	Monitoring Agent for Linux OS
ms	Tivoli Enterprise Monitoring Server
yn	IBM Tivoli Composite Application Manager Agent for WebSphere Applications

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Monitoring (WebSphere Business Monitor Business Space Console)"

Mit dem Test "Monitoring (WebSphere Business Monitor Business Space Console)" wird festgestellt, ob der Zugriff auf WebSphere Business Monitor Business Space über die HTTP-URL für WebSphere Business Monitor Business Space möglich ist.

Ressourcen

Für den Test "Monitoring (WebSphere Business Monitor Business Space Console)" wird die folgende Ressource verwendet:

- WebSphere Application Server (auf dem Anwendungsserver).

Fehlerbestimmung

Schlägt der Test "Monitoring (WebSphere Business Monitor Business Space Console)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Zugriffsproblem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Business Monitor-Protokolle:
      - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log`
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Anwendungsserversystem erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
3. Überprüfen Sie, ob der WebSphere Business Monitor-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:
   a. Melden Sie sich auf dem Anwendungsserversystem als `ibmadmin` an.
   b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *WAS-Administratorkennwort* aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh`. Wird die Nachricht `ADMU0508I: The Application Server "nodeagent" is STARTED.` (Der Anwendungsserver "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server nodeagent open for e-business; process id is 26654` (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).
   a. Wird die Nachricht `ADMU0509I: The Application Server "WBM_DE.AppTarget.WBMNode1.0" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "WBM_DE.AppTarget.WBMNode1.0" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM_DE.AppTarget.WBMNode1.0`. Wird die Nachricht `ADMU0508I: The Application Server "WBM_DE.AppTarget.WBMNode1.0" is STARTED.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie "WBM_DE.AppTarget.WBMNode1.0" starten mussten, wird eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server WBM_DE.AppTarget.WBMNode1.0 open for e-business; process id is 26654` (Server "WBM_DE.AppTarget.WBMNode1.0" für E-Business verfügbar; Prozess-ID ist 26654.).

   Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

   Starten Sie die Server in der folgenden Reihenfolge:
   a. nodeagent
   b. WBM_DE.AppTarget.WBMNode1.0

   Stoppen Sie die Server in der folgenden Reihenfolge:
   a. WBM_DE.AppTarget.WBMNode1.0
   b. nodeagent

Der Server "WBM_DE.AppTarget.WBMNode1.0" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh WBM_DE.AppTarget.WBMNode1.0 -username waswebadmin -password WAS-Administratorkennwort` ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS-Administratorkennwort` ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

4. Überprüfen Sie, ob der WebSphere Business Monitor-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung mithilfe der Administrationskonsole von WebSphere Application Server durch:
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://Anwendungsserver-Host:9060/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Anwendungsserver-Host* ist der Hostname für den Anwendungsserver.
   b. Überprüfen Sie den Status des Servers "WBM_DE.AppTarget.WBMNode1.0W", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

      Das Symbol zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

      Das Symbol zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

      Das Symbol zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Knotenagent (nodeagent) unter Umständen nicht aktiv. Sie können den Knotenagenten starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh` ausführen.

   Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

   Starten Sie die Server in der folgenden Reihenfolge:
   a. nodeagent
   b. WBM_DE.AppTarget.WBMNode1.0

   Stoppen Sie die Server in der folgenden Reihenfolge:
   a. WBM_DE.AppTarget.WBMNode1.0
   b. nodeagent

   Um den Server "WBM_DE.AppTarget.WBMNode1.0" zu stoppen, wählen Sie den Server aus und klicken Sie auf die entsprechende Option.

   Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS-Administratorkennwort` ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.
5. Überprüfen Sie, ob der Zugriff auf WebSphere Business Monitor Business Space vom WebSphere Portal-System auf dem Anwendungsserver aus über die URL `http://Anwendungsserver-Host:9084/BusinessSpace` möglich ist; dabei ist *Anwendungsserver-Host* der Hostname für den Anwendungsserver.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Monitoring (WebSphere Business Monitor Mobile Device Console)"

Mit dem Test "Monitoring (WebSphere Business Monitor Mobile Device Console)" wird festgestellt, ob der Zugriff auf WebSphere Business Monitor Mobile über die HTTP-URL von WebSphere Business Monitor Mobile möglich ist.

Ressourcen

Für den Test "Monitoring (WebSphere Business Monitor Mobile Device Console)" wird die folgende Ressource verwendet:

- WebSphere Application Server (auf dem Anwendungsserver).

Fehlerbestimmung

Schlägt der Test "Monitoring (WebSphere Business Monitor Mobile Device Console)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Zugriffsproblem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Business Monitor-Protokolle:
      - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log`
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Anwendungsserversystem erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
3. Überprüfen Sie, ob der WebSphere Business Monitor-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:
   a. Melden Sie sich auf dem Anwendungsserversystem als `ibmadmin` an.
   b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *WAS-Administratorkennwort* aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh`. Wird die Nachricht `ADMU0508I: The Application Server "nodeagent" is STARTED.` (Der Anwendungsserver "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server nodeagent open for e-business; process id is 26654` (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).
   a. Wird die Nachricht `ADMU0509I: The Application Server "WBM_DE.AppTarget.WBMNode1.0" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "WBM_DE.AppTarget.WBMNode1.0" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM_DE.AppTarget.WBMNode1.0`. Wird die Nachricht `ADMU0508I: The Application Server "WBM_DE.AppTarget.WBMNode1.0" is STARTED.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" wurde gestartet.) angezeigt, können Sie diesen Schritt über-

springen. Wenn Sie "WBM_DE.AppTarget.WBMNode1.0" starten mussten, wird eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server WBM_DE.AppTarget.WBMNode1.0 open for e-business; process id is 26654` (Server "WBM_DE.AppTarget.WBMNode1.0" für E-Business verfügbar; Prozess-ID ist 26654.).

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. WBM_DE.AppTarget.WBMNode1.0

Stoppen Sie die Server in der folgenden Reihenfolge:

a. WBM_DE.AppTarget.WBMNode1.0
b. nodeagent

Der Server "WBM_DE.AppTarget.WBMNode1.0" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh WBM_DE.AppTarget.WBMNode1.0 -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

4. Überprüfen Sie, ob der WebSphere Business Monitor-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung mithilfe der Administrationskonsole von WebSphere Application Server durch:
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://`*`Anwendungsserver-Host`*`:9060/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Anwendungsserver-Host* ist der Hostname für den Anwendungsserver.
   b. Überprüfen Sie den Status des Servers "WBM_DE.AppTarget.WBMNode1.0W", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

      Das Symbol zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

      Das Symbol zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

      Das Symbol zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Knotenagent (nodeagent) unter Umständen nicht aktiv. Sie können den Knotenagenten starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh` ausführen.

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. WBM_DE.AppTarget.WBMNode1.0

Stoppen Sie die Server in der folgenden Reihenfolge:

a. WBM_DE.AppTarget.WBMNode1.0
b. nodeagent

Um den Server "WBM_DE.AppTarget.WBMNode1.0" zu stoppen, wählen Sie den Server aus und klicken Sie auf die entsprechende Option.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Anwendungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

5. Überprüfen Sie, ob der Zugriff auf WebSphere Business Monitor Mobile vom WebSphere Portal-System auf dem Anwendungsserver aus über die URL `http://`*`Anwendungsserver-Host`*`:9084/mobile` möglich ist; dabei ist *Anwendungsserver-Host* der Hostname für den Anwendungsserver.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Policy (Tivoli Service Request Manager Maximo Console)"

Mit dem Test "Policy (Tivoli Service Request Manager Maximo Console)" wird festgestellt, ob der Zugriff auf Tivoli Service Request Manager Maximo über die Startcenterseite von Tivoli Service Request Manager Maximo möglich ist.

Ressourcen

Für den Test "Policy (Tivoli Service Request Manager Maximo Console)" wird die folgende Ressource verwendet:

- Tivoli Service Request Manager Maximo (auf dem Ereignisserver).

Fehlerbestimmung

Schlägt der Test "Policy (Tivoli Service Request Manager Maximo Console)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Zugriffsproblem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Ereignisserver die folgenden Tivoli Service Request Manager-Protokolle:
      - `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log`
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf den Ereignisserver- und Anwendungsserversystemen erreicht wurde (dies kann mit dem Befehl **`df -h`** festgestellt werden).
3. Überprüfen Sie, ob der Tivoli Service Request Manager-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung manuell durch:
   a. Melden Sie sich auf dem Ereignisserversystem als `ibmadmin` an.
   b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/serverStatus.sh -all -username waswebadmin -password` *`WAS-Administratorkennwort`* aus. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "WBM_DE.AppTarget.WBMNode1.0" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie den Server "nodeagent" mit dem Befehl `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh`. Wird die Nachricht `ADMU0508I: The Application Server "nodeagent" is STARTED.` (Der Anwendungs-

server "nodeagent" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "nodeagent" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server nodeagent open for e-business; process id is 26654` (Server "nodeagent" für E-Business verfügbar; Prozess-ID ist 26654).

a. Wird die Nachricht `ADMU0509I: The Application Server "MXServer1" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "cpudServer1" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "MXServer1" mit dem Befehl `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startServer.sh MXServer1`. Wird die Nachricht `ADMU0508I: The Application Server "MXServer1" is STARTED.` (Der Anwendungsserver "MXServer1" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "MXServer1" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server MXServer1 open for e-business; process id is 26654` (Server "MXServer1" ist für E-Business verfügbar; Prozess-ID ist 26654).

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. MXServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. MXServer1
b. nodeagent

Der Server "MXServer1" wird gestoppt, indem in einem Befehlsfenster auf dem Ereignisserver der Befehl `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopServer.sh MXServer1 -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Ereignisserver der Befehl `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

4. Überprüfen Sie, ob der Tivoli Service Request Manager-Server gestartet wurde. Dies kann entweder mithilfe der Administrationskonsole von WebSphere Application Server oder aber manuell festgestellt werden. So führen Sie diese Prüfung mithilfe der Administrationskonsole von WebSphere Application Server durch:
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server unter `http://`*`Ereignisserver-Host`*`:9061/admin` mit der Verwaltungs-ID "admin" und dem Administratorkennwort von WebSphere Application Server an. *Ereignisserver-Host* ist der Hostname für den Ereignisserver.
   b. Überprüfen Sie den Status des Servers "MXServer1", indem Sie auf **Servers** > **Server Types** > **WebSphere application servers** (Server > Servertypen > WebSphere-Anwendungsserver) klicken.

      Das Symbol  zeigt an, dass der Server gestartet wurde. Wählen Sie ggf. den Server aus und starten Sie ihn erneut, indem Sie auf die entsprechende Option klicken.

      Das Symbol  zeigt an, dass der Server gestoppt wurde. Wählen Sie den Server aus und starten Sie ihn, indem Sie auf die entsprechende Option klicken.

      Das Symbol  zeigt an, dass der Server nicht verfügbar ist. In diesem Fall ist der Knotenagent (nodeagent) unter Umständen nicht aktiv. Sie können den Knotenagenten starten, indem Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh` ausführen.

Wichtig: Die Server müssen in einer vorgegebenen Reihenfolge gestartet bzw. gestoppt werden.

Starten Sie die Server in der folgenden Reihenfolge:

a. nodeagent
b. MXServer1

Stoppen Sie die Server in der folgenden Reihenfolge:

a. MXServer1
b. nodeagent

Um den Server "MXServer1" zu stoppen, wählen Sie den Server aus und klicken Sie auf auf die entsprechende Option.

Der Server "nodeagent" wird gestoppt, indem in einem Befehlsfenster auf dem Ereignisserver der Befehl `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password` *`WAS-Administratorkennwort`* ausgeführt wird. Dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.

5. Überprüfen Sie, ob der Zugriff auf die Startcenterseite von Tivoli Service Request Manager Maximo vom WebSphere Portal-System auf dem Ereignisserver aus über die URL `http://`*`Ereignisserver-Host`*`:31015/maximo/ui/login` möglich ist; dabei ist *Ereignisserver-Host* der Hostname für den Ereignisserver. Die Benutzer-ID ist `maxadmin`.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Security (Tivoli Access Manager)"

Mit dem Test "Security (Tivoli Access Manager)" wird festgestellt, ob Tivoli Access Manager aktiv ist; dazu wird vom Verwaltungsserver aus der Befehl **`pd_start`** gesendet und das Ergebnis anschließend überprüft.

Ressourcen

Für den Test "Security (Tivoli Access Manager)" wird die folgende Ressource verwendet:

- Tivoli Access Manager, einschließlich der Richtlinien- und Berechtigungsserver (auf dem Verwaltungsserver)

Fehlerbestimmung

Schlägt der Test "Security (Tivoli Access Manager)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Informationen zu diesem Vorgang

In den im Folgenden beschriebenen Schritten ist der Tivoli Access Manager-Autorisierungsserver "pdmgrproxyd" der Richtlinien-Proxy-Server und "webseald-default" der Tivoli Access Manager-WebSEAL-Server.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Verwaltungsserver die folgenden Tivoli Access Manager-Protokolle:
      - `/var/PolicyDirector/log/msg__pdmgrd_utf8.log`
      - `/var/PolicyDirector/log/msg__pdacld_utf8.log`
   b. Überprüfen Sie auf dem Anwendungsserver die folgenden Tivoli Access Manager-Protokolle:
      - `/var/pdweb/log/msg__*.log` (* ist ein beliebiger Wert)
      - `/var/pdweb/log/config_data__*.log` (* ist ein beliebiger Wert)

2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf den Verwaltungsserver- und Anwendungsserversystemen erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
3. Überprüfen Sie, ob die erforderlichen Tivoli Access Manager-Komponenten aktiv sind.
   a. Melden Sie sich auf dem Verwaltungsserver als `root` an einer Terminalsitzung an.
   b. Führen Sie den Befehl **pd_start status** aus. Das Ergebnis ist ähnlich dem folgenden Beispiel:

```
Tivoli Access Manager servers

Server         Enabled   Running
---------------------------------
pdmgrd           yes       yes
pdacld           yes       yes
pdmgrproxyd      no        no
```

   c. Ist der Server "pdmgrd" oder "pdacld" nicht aktiv, starten Sie diese Server mit dem Befehl **pd_start start**.

      Anmerkung: Auf dem Verwaltungsserver sind nur die Server "pdmgrd" und "pdacld" aktiviert. Beide werden mit dem Befehl **pd_start start** gestartet und können mit dem Befehl **pd_start stop** gestoppt werden.
4. Überprüfen Sie, ob die erforderlichen Tivoli Access Manager WebSEAL-Komponenten aktiv sind.
   a. Melden Sie sich auf dem Anwendungsserver als Rootbenutzer an einer Terminalsitzung an.
   b. Führen Sie den Befehl **pd_start status** aus. Das Ergebnis ist ähnlich dem folgenden Beispiel:

```
Tivoli Access Manager servers

Server         Enabled   Running
---------------------------------
pdmgrd           no        no
pdacld           no        no
pdmgrproxyd      no        no
webseald-default yes       yes
```

   c. Ist der Server "webseald-default" nicht aktiv, starten Sie ihn mit dem Befehl **pd_start start**.

      Anmerkung: Auf dem Anwendungsserver ist nur der Server "webseald-default" aktiviert. Er wird mit dem Befehl **pd_start start** gestartet und kann mit dem Befehl **pd_start stop** gestoppt werden.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Security (Tivoli Access Manager Web Portal Manager)"

Mit dem Test "Security (Tivoli Access Manager Web Portal Manager)" wird festgestellt, ob die Tivoli Access Manager-Webportalanwendung über die URL der Tivoli Access Manager-Webportalanwendung erreicht werden kann.

Ressourcen

Für den Test "Security (Tivoli Access Manager Web Portal Manager)" wird die folgende Ressource verwendet:

- Tivoli Access Manager - Web Portal Manager (auf dem Verwaltungsserver).

Fehlerbestimmung

Schlägt der Test "Security (Tivoli Access Manager Web Portal Manager)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Zugriffsproblem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden WebSphere Portal-Protokolle:
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
   b. Überprüfen Sie auf dem Verwaltungsserver die folgenden Tivoli Access Manager - WebSphere Portal Manager-Protokolle:
      - `/opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log`
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf dem Verwaltungsserversystem erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
3. Überprüfen Sie, ob Tivoli Access Manager - Web Portal Manager gestartet wurde.
   a. Melden Sie sich auf dem Verwaltungsserver als `ibmadmin` an.
   b. Führen Sie in einem Befehlsfenster den Befehl `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/serverStatus.sh -all -username waswebadmin -password` *WAS-Administratorkennwort* aus; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere Application Server-Administrators.
   c. Wird die Nachricht `ADMU0509I: The Application Server "dmgr" cannot be reached. It appears to be stopped.` (Der Anwendungsserver "dmgr" kann nicht erreicht werden. Er wurde möglicherweise gestoppt.) angezeigt, starten Sie "dmgr" mit dem Befehl `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/startManager.sh`. Wird die Nachricht `ADMU0508I: The Application Server "dmgr" is STARTED.` (Der Anwendungsserver "dmgr" wurde gestartet.) angezeigt, können Sie diesen Schritt überspringen. Wenn Sie den Server "dmgr" starten mussten, wird anschließend eine Nachricht ähnlich der folgenden angezeigt: `ADMU3000I: Server dmgr open for e-business; process id is 26654` (Server "dmgr" ist für E-Business verfügbar; Prozess-ID ist 26654).

   WebSphere Application Server Deployment Manager, einschließlich Tivoli Access Manager - Web Portal Manager, wird gestoppt, indem in einem Befehlsfenster auf dem Verwaltungsserver der Befehl `/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/stopManager.sh -username waswebadmin -password` *WAS-Administratorkennwort* ausgeführt wird; dabei ist *WAS-Administratorkennwort* das Kennwort des WebSphere-Administrators.
4. Überprüfen Sie, ob vom WebSphere Portal-System aus ein Zugriff auf Tivoli Access Manager - Web Portal Manager möglich ist.
   a. Rufen Sie auf dem Verwaltungsserver die URL `http://`*Verwaltungsserver-Host*`9060/admin` auf; dabei ist *Verwaltungsserver-Host* der Hostname für den Verwaltungsserver.
   b. Klicken Sie auf **Tivoli Access Manager** > **Web Portal Manager** > **Users** > **Search Users** (Tivoli Access Manager > Web Portal Manager > Benutzer > Nach Benutzern suchen).
   c. Melden Sie sich als Benutzer `sec_master` an.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Security (WebSEAL Console)"

Mit dem Test "Security (WebSEAL Console)" wird festgestellt, ob Tivoli Access Manager und Tivoli Access Manager WebSEAL mit den erforderlichen Ressourcen aktiv sind; dazu wird die HTTP-URL für WebSEAL an Port 80 aufgerufen und überprüft, ob die zurückgegebene Seite die Zeichenfolge "Intelligent Operations Center" enthält.

Ressourcen

Für den Test "Security (WebSEAL Console)" werden die folgenden Ressourcen verwendet:

- Tivoli Access Manager, einschließlich der Richtlinien- und Berechtigungsserver (auf dem Verwaltungsserver)

- Tivoli Access Manager WebSEAL (auf dem Anwendungsserver)

Fehlerbestimmung

Schlägt der Test "Security (WebSEAL Console)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Informationen zu diesem Vorgang

In den im Folgenden beschriebenen Schritten ist der Tivoli Access Manager-Autorisierungsserver "pdmgrproxyd" der Richtlinien-Proxy-Server und "webseald-default" der Tivoli Access Manager-WebSEAL-Server.

Vorgehensweise

1. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Verwaltungsserver die folgenden Tivoli Access Manager-Protokolle:
      - `/var/PolicyDirector/log/msg__pdmgrd_utf8.log`
      - `/var/PolicyDirector/log/msg__pdacld_utf8.log`
   b. Überprüfen Sie auf dem Anwendungsserver die folgenden Tivoli Access Manager-Protokolle:
      - `/var/pdweb/log/msg__*.log` (* ist ein beliebiger Wert)
      - `/var/pdweb/log/config_data__*.log` (* ist ein beliebiger Wert)
2. Überprüfen Sie, ob die Kapazität der Dateisysteme auf den Verwaltungsserver- und Anwendungsserversystemen erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
3. Überprüfen Sie, ob die erforderlichen Tivoli Access Manager-Komponenten aktiv sind.
   a. Melden Sie sich auf dem Verwaltungsserver als `root` an einer Terminalsitzung an.
   b. Führen Sie den Befehl **pd_start status** aus. Das Ergebnis ist ähnlich dem folgenden Beispiel:

```
Tivoli Access Manager servers

Server         Enabled   Running
---------------------------------
pdmgrd           yes       yes
pdacld           yes       yes
pdmgrproxyd      no        no
```

   c. Ist der Server "pdmgrd" oder "pdacld" nicht aktiv, starten Sie diese Server mit dem Befehl **pd_start start**.

      Anmerkung: Auf dem Verwaltungsserver sind nur die Server "pdmgrd" und "pdacld" aktiviert. Beide werden mit dem Befehl **pd_start start** gestartet und können mit dem Befehl **pd_start stop** gestoppt werden.
4. Überprüfen Sie, ob die erforderlichen Tivoli Access Manager WebSEAL-Komponenten aktiv sind.
   a. Melden Sie sich auf dem Anwendungsserver als Rootbenutzer an einer Terminalsitzung an.
   b. Führen Sie den Befehl **pd_start status** aus. Das Ergebnis ist ähnlich dem folgenden Beispiel:

```
Tivoli Access Manager servers

Server         Enabled   Running
---------------------------------
pdmgrd           no        no
pdacld           no        no
pdmgrproxyd      no        no
webseald-default yes       yes
```

   c. Ist der Server "webseald-default" nicht aktiv, starten Sie ihn mit dem Befehl **pd_start start**.

      Anmerkung: Auf dem Anwendungsserver ist nur der Server "webseald-default" aktiviert. Er wird mit dem Befehl **pd_start start** gestartet und kann mit dem Befehl **pd_start stop** gestoppt werden.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Web Server (IBM HTTP Server Console)"

Mit dem Test "Web Server (IBM HTTP Server Console)" wird der Zugriff auf IBM HTTP Server über die IBM HTTP Server-URL überprüft.

Ressourcen

Für den Test "Web Server (IBM HTTP Server Console)" wird die folgende Ressource verwendet:

- IBM HTTP Server (auf dem Anwendungsserver).

Fehlerbestimmung

Schlägt der Test "Web Server (IBM HTTP Server Console)" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Problem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob eine Netzverbindung zum Anwendungsserver besteht. Dazu können **ping**-Befehle mit dem kurzen und dem vollständig qualifizierten Hostnamen des Anwendungsservers gesendet werden. Aus dem Ergebnis dieser **ping**-Befehle geht hervor, ob der Hostname vom DNS oder von der Datei `/etc/hosts` korrekt aufgelöst wird.
2. Überprüfen Sie die Protokolldateien auf Laufzeitausnahmebedingungen.
   a. Überprüfen Sie auf dem Anwendungsserver die folgenden IBM HTTP-Protokolle:
      - `/opt/IBM/HTTPServer/logs/error_log`
      - `/opt/IBM/HTTPServer/logs/access_log`
3. Überprüfen Sie, ob die Kapazität des Dateisystems auf dem Anwendungsserver erreicht wurde (dies kann mit dem Befehl **df -h** festgestellt werden).
4. Überprüfen Sie, ob vom WebSphere Portal-System aus der Zugriff auf die Standardseite von IBM HTTP Server möglich ist.
   a. Rufen Sie auf dem Anwendungsserver `https://`*Anwendungsserver-Host*`:82/` auf; dabei ist *Anwendungsserver-Host* der Hostname des Anwendungsservers.
   b. Ist kein Zugriff auf die Standardseite möglich, führen Sie den Befehl **ps -ef | grep HTTPServer** aus, um festzustellen, ob die IBM HTTP Server-Prozesse aktiv sind. Die Namen der IBM HTTP Server-Prozesse beginnen mit `/opt/IBM/HTTPServer/bin/httpd`. Insgesamt gibt es sieben Prozesse.
   c. Sind nur einige Prozesse aktiv, müssen Sie die aktiven Prozesse zunächst stoppen und anschließend alle Prozesse erneut starten.
      1) Melden Sie sich auf dem Anwendungsserver als Benutzer `root` an.
      2) Wechseln Sie in das Verzeichnis `/opt/IBM/HTTPServer/bin`.
      3) Führen Sie die folgenden Befehle aus, um alle IBM HTTP Server-Prozesse zu stoppen:
         ```
         ./apachectl stop
         ./adminctl stop
         ```
      4) Überprüfen Sie mit dem Befehl **ps -ef | grep HTTPServer**, ob alle Prozesse gestoppt wurden.
      5) Sind einige IBM HTTP Server-Prozesse immer noch aktiv, müssen Sie sie mit dem Befehl **kill -9** *Prozess-ID* stoppen; dabei ist *Prozess-ID* die Prozess-ID des IBM HTTP Server-Prozesses.
   d. Sind die HTTP Server-Prozesse nicht (mehr) aktiv, starten Sie die IBM HTTP Server-Komponenten.
      1) Melden Sie sich am Anwendungsserver als `root` an.
      2) Wechseln Sie in das Verzeichnis `/opt/IBM/HTTPServer/bin`.
      3) Führen Sie die folgenden Befehle aus, um alle IBM HTTP Server-Prozesse zu starten:
         ```
         ./adminctl start
         ./apachectl start
         ```

4) Überprüfen Sie mit dem Befehl **ps -ef | grep HTTPServer**, ob alle Prozesse gestartet wurden.

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Intelligent Operations Center Event Flow"

Mit dem Test "Intelligent Operations Center Event Flow" wird festgestellt, ob die kritischen Komponenten in Zusammenhang mit den IBM Intelligent Operations Center-Ereignisprozessen wie erwartet arbeiten. Dazu werden externe Ereignisse simuliert; anschließend wird überprüft, ob die Ergebnisse den Erwartungen entsprechen.

Ressourcen

Für den Test "Intelligent Operations Center Event Flow" werden die folgenden Ressourcen verwendet:

- IBM WebSphere Message Broker (auf dem Anwendungsserver).
- IBM WebSphere Message Queue (auf dem Anwendungsserver).
- IBM Netcool/OMNIbus (auf dem Ereignisserver).
- IBM Netcool/Impact (auf dem Ereignisserver).
- IBM DB2 (auf dem Datenserver).

Fehlerbestimmung

Schlägt der Test "Intelligent Operations Center Event Flow" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Zugriffsproblem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob die IBM Intelligent Operations Center-Komponenten aktiv sind.
   a. Führen Sie in einem Befehlsfenster auf dem Verwaltungsserver den Befehl **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status all** *Kennwort* aus; dabei ist *Kennwort* das Kennwort des IBM Intelligent Operations Center-Administrators, das bei der Implementierung von IBM Intelligent Operations Center definiert wurde.
   b. Sind einige Komponenten nicht aktiv, starten Sie sie mit dem Befehl **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start** *Komponenten-ID Kennwort*; dabei ist *Kennwort* das IBM Intelligent Operations Center-Administratorkennwort, das bei der Implementierung von IBM Intelligent Operations Center definiert wurde, und *Komponenten-ID* eine ID, die bei Ausführung von **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh help** unter `Target Options` (Zieloptionen) aufgelistet ist.
2. Überprüfen Sie das Netcool/OMNIbus-Protokoll (`/opt/IBM/netcool/omnibus/log/ioc_xml.log`) auf dem Ereignisserver auf Fehler.
3. Starten Sie gegebenenfalls den Tivoli Netcool/OMNIbus-Testmonitor, indem Sie auf dem Ereignisserver den folgenden Befehl ausführen:

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Test "Intelligent Operations Center Notification Flow"

Mit dem Test "Intelligent Operations Center Notification Flow" wird festgestellt, ob die kritischen Komponenten in Zusammenhang mit den IBM Intelligent Operations Center-Benachrichtigungsprozessen wie erwartet arbeiten. Dazu werden externe Benachrichtigungen simuliert; anschließend wird überprüft, ob die Ergebnisse den Erwartungen entsprechen.

Ressourcen

Für den Test "Intelligent Operations Center Notification Flow" werden die folgenden Ressourcen verwendet:

- IBM WebSphere Message Queue (auf dem Anwendungsserver).
- IBM Netcool/OMNIbus (auf dem Ereignisserver).
- IBM Netcool/Impact (auf dem Ereignisserver).
- IBM DB2 (auf dem Datenserver).

Fehlerbestimmung

Schlägt der Test "Intelligent Operations Center Notification Flow" fehl, gehen Sie wie im Folgenden beschrieben vor, um das Zugriffsproblem zu identifizieren und zu beheben.

Vorgehensweise

1. Überprüfen Sie, ob die IBM Intelligent Operations Center-Komponenten aktiv sind.
   a. Führen Sie in einem Befehlsfenster auf dem Verwaltungsserver den Befehl **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status all** *Kennwort* aus; dabei ist *Kennwort* das Kennwort des IBM Intelligent Operations Center-Administrators, das bei der Implementierung von IBM Intelligent Operations Center definiert wurde.
   b. Sind einige Komponenten nicht aktiv, starten Sie sie mit dem Befehl **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start** *Komponenten-ID Kennwort*; dabei ist *Kennwort* das IBM Intelligent Operations Center-Administratorkennwort, das bei der Implementierung von IBM Intelligent Operations Center definiert wurde, und *Komponenten-ID* eine ID, die bei Ausführung von **/opt/IBM/ISP/mgmt/scripts/IOCControl.sh help** unter `Target Options` (Zieloptionen) aufgelistet ist.
2. Überprüfen Sie das Netcool/OMNIbus-Protokoll (`/opt/IBM/netcool/omnibus/log/ioc_xml.log`) auf dem Ereignisserver auf Fehler.
3. Starten Sie gegebenenfalls den Tivoli Netcool/OMNIbus-Testmonitor, indem Sie auf dem Ereignisserver den folgenden Befehl ausführen:

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```

Nächste Schritte

Beheben Sie alle Probleme oder Fehler, die aufgetreten sind, und wiederholen Sie den Test.

Kapitel 7. Lösung pflegen

Führen Sie die in diesem Abschnitt beschriebenen Aufgaben aus, damit Ihre Lösung stets problemlos genutzt werden kann.

Daten sichern

Um den Verlust von geschäftskritischen Daten in IBM Intelligent Operations Center zu vermeiden, sichern Sie bestimmte Dateien, Verzeichnisse und Datenbanken in regelmäßigen Zeitabständen.

Wenn Sie IBM Intelligent Operations Center erweitern, wird empfohlen, eine Sicherungsprozedur für die hinzugefügten Elemente zu entwickeln, wie z. B.:

- Berichte
- Zusätzliche Datenbanken
- Datenbanktabellen
- Benutzerdefinierte Analyse
- Portlets
- Java-Anwendungen

Berücksichtigen Sie auch Daten, die Sie kumuliert haben, z. B.:

- CAP-Datenbankdaten (Common Access Protocol)
- IBM WebSphere Business Monitor-Datenbankdaten
- Daten der LDAP-Benutzerregistry (Lightweight Directory Access Protocol)
- GIS-Daten (Geographical Information System)

Verwenden Sie eine Namenskonvention, damit die hinzugefügten Erweiterungen einfacher identifiziert werden können. Verfolgen Sie die Daten, die Sie seit der Installation der ursprünglichen Lösung erstellt oder kumuliert haben. Implementieren Sie Prozeduren zum Sichern der Daten, sodass beim Upgrade der Lösung keine geschäftskritischen Daten verloren gehen.

Datenbanken sichern

In der folgenden Tabelle sind die Datenbanken aufgelistet, deren Sicherung in IBM Intelligent Operations Center empfohlen wird.

Tabelle 80. IBM Intelligent Operations Center-Datenbanken

Service oder Komponente	Datenbankinstanz	Datenbanknamen	Server
Intelligent Operations Center-Datenbank	db2inst1	• IOCDB	Datenserver
Portal	db2inst2	• CUSTDB • FDBKDB • LKMDDB • JCRDB • COMMDB • RELDB	Datenserver
Business Intelligence	db2inst3	• CXLOGDB • CXCONTDB	Datenserver

Tabelle 80. IBM Intelligent Operations Center-Datenbanken (Forts.)

Service oder Komponente	Datenbankinstanz	Datenbanknamen	Server
Geschäftsregel- und Geschäftsaktivität-Monitor	db2inst4	• UDDIDB • WODMDCDB • MONITOR • WBMDB • RESDB	Datenserver
Semantikmodell	db2inst5	• JTS • IIC	Datenserver
Serviceanforderungs-management	db2inst6	• MAXIMO	Datenserver
Identitätsmanagement	db2inst7	• TIMDB	Datenserver
Anwendungen	db2inst8	• LDAPDB • LDAPDB2B	Datenserver

Momentaufnahmen der virtuellen Infrastruktur erstellen

Die meisten virtuellen Infrastrukturen verfügen über eine Funktion zur Momentaufnahme, die den Status und die Daten Ihrer virtuellen Umgebung zu einem bestimmten Zeitpunkt speichert. Es wird dringend empfohlen, dass Sie eine Momentaufnahme Ihrer Umgebung erstellen, bevor Sie größere Änderungen vornehmen. Es stehen viele Tools zum Management der virtuellen Infrastruktur zur Verfügung, von denen die meisten über ihre eigene Implementierung einer Funktion zur Momentaufnahme verfügen. Es ist wichtig, sich mit den speziellen Anforderungen und Anweisungen zur ordnungsgemäßen Sicherung Ihrer virtuellen Umgebung vertraut zu machen, indem Sie die Anweisungen im vom Anbieter der virtuellen Infrastruktur bereitgestellten Verwaltungshandbuch sorgfältig lesen.

Zugehörige Tasks:

„Vor der Anpassung von KPIs Sicherung durchführen” auf Seite 182
Sichern und stellen Sie KPIs wieder her, die mit IBM WebSphere Business Monitor oder mit dem Portlet "Key Performance Indicators (KPIs)" erstellt oder geändert wurden.

Zugehörige Informationen:

Redbooks für IBM Smarter Cities Software Solutions

Leistung optimieren

In den folgenden Abschnitten wird beschrieben, wie Sie die Leistung von Anwendungsserver und WebSphere Application Server optimieren.

Zugehörige Informationen:

Handbuch zur Leistungsoptimierung für IBM Websphere Portal V 7.0

Information Center für IBM Websphere Application Server, Network Deployment, Version 7.0

Anwendungsserver optimieren

Informationen zu diesem Vorgang

Verwenden Sie die folgenden Richtlinien, die auf den Ergebnissen von Leistungstests basieren, um die Größe des Heapspeichers der Java Virtual Machine festzulegen.

Vorgehensweise

1. Setzen Sie die Mindestgröße und die maximale Größe des Heapspeichers auf dieselben Werte.
2. Setzen Sie die Größe des Heapspeichers auf einen Wert, der mit dem physischen Speicher kompatibel ist und größer als 2 GB ist.

Nächste Schritte

Weitere Informationen erhalten Sie über den entsprechenden Link am Ende des Themas.

WebSphere Application Server optimieren

Weitere Informationen zur Optimierung der Leistung von WebSphere Application Server Version 7 erhalten Sie über den entsprechenden Link am Ende des Themas.

Protokolldateien verwalten

IBM Intelligent Operations Center speichert Protokolldateien in mehreren verschiedenen Verzeichnissen. Um Probleme mit der Systemleistung zu vermeiden, müssen Sie Protokolldateien in regelmäßigen Abständen archivieren und die ursprünglichen Protokolldateien entfernen.

Wenn Sie Protokolldateien nicht verwalten und die Anzahl der Protokolldateien unbegrenzt steigt, belegen die Protokolldateien irgendwann möglicherweise eine ganze Dateisystempartition. Die Belegung einer ganzen Dateisystempartition hat möglicherweise negative Auswirkungen und kann dazu führen, dass das System gestoppt wird.

Weitere Informationen zu Protokolldateien, die in IBM Intelligent Operations Center verfügbar sind, erhalten Sie über den Link am Ende des Themas.

Zugehörige Konzepte:

„Fehlersuche in den Komponenten” auf Seite 317
Sie können das Tool "Systemprüfung" für die Suche von Komponentenfehlern im IBM Intelligent Operations Center verwenden.

LTPA-Token für Single Sign-on aktualisieren

IBM Intelligent Operations Center verwendet ein Lightweight Third-Party Authentication-Token (LTPA-Token), um Single Sign-on für mehrere Services zu aktivieren. Die Token und Schlüssel, die während der Installation generiert wurden, verfallen nicht. Es ist ein bewährtes Sicherheitsverfahren, in regelmäßigen Abständen ein LTPA-Token neu zu generieren und die Services, die es verwenden, zu aktualisieren.

Vorbereitende Schritte

Das IBM Intelligent Operations Center-Produkt muss installiert und alle Services gestartet sein, bevor das LTPA-Token aktualisiert wird.

Dieses Verfahren erfordert, dass alle Services gestoppt und gestartet werden. Die Aktualisierung sollte also nicht vorgenommen werden, während das System aktiv ist. Alle Benutzer, die auf dem System angemeldet sind, sind von einer Serviceunterbrechung betroffen und können Daten verlieren.

Vorgehensweise

Generieren Sie ein neues LTPA-Token für den Anwendungsserver

1. Öffnen Sie auf dem Anwendungsserver einen Web-Browser und gehen Sie zu `http://`*`Anwendungshost`*`:9060/ibm/console`, wobei *Anwendungshost* der Hostname der Anwendungsserver ist.
2. Melden Sie sich als Benutzer `webwasadmin` mit dem Kennwort an, dass im Parameter `WAS.ADMIN.ACCOUNT.PWD` der Datei mit den Topologieeigenschaften festgelegt wurde.

3. Klicken Sie auf **Sicherheit** > **Globale Sicherheit** > **Authentifizierungsmechanismen und Verfallsdatum** > **LTPA** > **Schlüssel generieren**.
4. Geben Sie für das neue LTPA-Token ein Kennwort zweimal ein. Das Kennwort wird verwendet, um das LTPA-Token zu verschlüsseln. Dieses Kennwort wird bei Import des LTPA-Tokens verwendet. Tragen Sie das Kennwort als ParameterWAS.LTPA.PWD in die Datei mit den Topologieeigenschaften ein.
5. Geben Sie den Pfad und den Dateinamen ein, wo das LTPA-Token gespeichert wird, z. B. /tmp/newapp.ltpa. Wenn Sie einen anderen Pfad oder Dateinamen angeben, ersetzen Sie in den verbleibenden Schritten Ihren Pfad und Dateinamen mit /tmp/newapp.ltpa.
6. Klicken Sie auf **Schlüssel exportieren**. Das neue LTPA-Token wird als /tmp/newapp.ltpa gespeichert.
7. Klicken Sie auf **Nachrichten** > **Speichern**. Aktualisierungen werden gespeichert. Ignorieren Sie Warnmeldungen darüber, dass die Single Sign-on-Domäne nicht definiert ist.

Kopieren Sie das neue LTPA-Token in den Ereignisserver.

8. Melden Sie sich auf dem Anwendungsserver als root-Benutzer an und öffnen Sie ein Terminalfenster.
9. Führen Sie den Befehl **cp /tmp/newapp.ltpa /tmp/stproxy.ltpa** aus. Mit diesem wird die Datei ersetzt, die erstellt wurde, als IBM Intelligent Operations Center installiert wurde.
10. Führen Sie den Befehl **scp /tmp/newapp.ltpa root@***Ereignishost* **:/tmp/newapp.ltpa** aus, wo *Ereignishost* der Hostname des Ereignisserver ist. Geben Sie, wenn Sie dazu aufgefordert werden, das root-Kennwort für den Ereignisserver ein. Das neue LTPA-Token wird auf den Ereignisserver kopiert.

Importieren Sie das neue LTPA-Token

11. Öffnen Sie auf dem Ereignisserver einen Web-Browser und gehen Sie zu http://*Ereignishost*:9061/ibm/console, wobei *Ereignishost* der vollständig qualifizierte Hostname des Ereignisserver ist.
12. Melden Sie sich als Benutzer webwasadmin mit dem Kennwort an, das im Parameter WAS.ADMIN.ACCOUNT.PWD der Datei mit den Topologieeigenschaften festgelegt wurde.
13. Klicken Sie auf **Sicherheit** > **Sichere Verwaltung, Anwendungen und Infrastruktur** > **Authentifizierungsmechanismen und Verfallsdatum**.
14. Geben Sie das Kennwort für das LTPA-Token und /tmp/newapp.ltpa als Dateinamen ein.
15. Klicken Sie auf **Schlüssel importieren**.
16. Klicken Sie auf **Nachrichten** > **Speichern**. Aktualisierungen werden gespeichert.

Generieren Sie ein neues LTPA-Token für den Ereignisserver

17. Klicken Sie auf **Authentifizierungsmechanismen und Verfallsdatum** > **Schlüssel generieren**.
18. Geben Sie für das neue LTPA-Token ein Kennwort zweimal ein. Dieses Kennwort wird bei Import des LTPA-Tokens verwendet.
19. Geben Sie den Pfad und den Dateinamen ein, wo das LTPA-Token gespeichert wird, z. B. /tmp/newevent.ltpa. Wenn Sie einen anderen Pfad oder Dateinamen angeben, ersetzen Sie in den verbleibenden Schritten Ihren Pfad und Dateinamen mit /tmp/newevent.ltpa.
20. Klicken Sie auf **Schlüssel exportieren**. Das neue LTPA-Token wird als /tmp/newevent.ltpa gespeichert.

Kopieren Sie das neue Ereignisserver LTPA-Token auf den Anwendungsserver.

21. Melden Sie sich auf dem Anwendungsserver als root-Benutzer an und öffnen Sie ein Terminalfenster.
22. Führen Sie den Befehl **scp /tmp/newevent.ltpa root@***Ereignishost* **:/tmp/newevent.ltpa** aus, wobei *Ereignishost* der Hostname des Ereignisserver ist. Geben Sie, wenn Sie dazu aufgefordert werden, das root-Kennwort für den Ereignisserver ein. Das LTPA-Token wird auf den Ereignisserver kopiert.

Aktualisieren Sie den Sicherheitsservice mit dem neuen LTPA-Token.

23. Melden Sie sich am Anwendungsserver als root-Benutzer an und öffnen Sie ein Terminalfenster.
24. Führen Sie den Befehl **cp /tmp/newapp.ltpa /opt/pdweb/etc/** aus.
25. Führen Sie den Befehl **cp /tmp/newevent.ltpa /opt/pdweb/etc/** aus.
26. Erstellen Sie eine Befehlsdatei mit dem Namen /tmp/pd.com, die die folgenden Befehle enthält:

```
server task
default-webseald-Anwendungshost
create -t tcp -h Anwendungshost
-p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebclient
server task
default-webseald-Anwendungshost
create -t tcp -h Anwendungshost
-p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stbaseapi
server task
default-webseald-Anwendungshost
create -t tcp -h
Anwendungshost -p
9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebapi
server task
default-webseald-Anwendungshost
create -t tcp -h
Anwendungshost
-p 9081 -b
supply -c iv-user,iv-creds -i -j -f -J trailer -A -2 -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw
/cognosserver task
default-webseald-Anwendungshost
create -t tcp -h Ereignishost
-p 82 -i
-j -f -J trailer -A -2 -F /opt/pdweb/etc/newevent.ltpa -Z eventLTPApw /tsrm
```

Dabei gilt Folgendes:

Anwendungshost
: ist der vollständig qualifizierte Hostname des Anwendungsserver.

Ereignishost
: ist der vollständig qualifizierte Hostname des Ereignisserver.

appLTPApw
: ist das Kennwort, das bei Erstellung des LTPA-Tokens für den Anwendungsserver festgelegt wurde.

eventLTPApw
: ist das Kennwort, das bei Erstellung des LTPA-Tokens für den Ereignisserver festgelegt wurde.

27. Führen Sie den Befehl **/opt/PolicyDirector/bin/pdadmin -a sec_master -p***Kennwort* **/ tmp/pd.com** aus, wobei *Kennwort* das im Parameter TAM.WEBSEAL.ADMIN.PWD der Datei mit den Topologieeigenschaften definierte Kennwort ist.

Single Sign-on für den Service zur Zusammenarbeit aktualisieren.

28. Folgen Sie den Schritten in „Single Sign-on für Services zur Zusammenarbeit konfigurieren” auf Seite 57, um Single Sign-on für den Service zur Zusammenarbeit zu aktualisieren.

Stoppen Sie alle Services und starten Sie sie neu.

29. Stoppen Sie mithilfe des Plattformsteuerungstool alle Services.
30. Starten Sie mithilfe des Plattformsteuerungstool alle Services. LTPA-Token werden an alle Services weitergegeben.

Wartungstipps

Zusätzliche Tipps zum Warten der Lösung sind in Form von einzelnen Technotes im IBM Support Portal dokumentiert.

Mit dem folgenden Link wird eine angepasste Anfrage bei der Wissensdatenbank für den Live-Support für alle Versionen von IBM Intelligent Operations Center gestartet: View all maintenance tips for IBM Intelligent Operations Center.

Kapitel 8. Benutzerschnittstelle der Lösung verwenden

IBM Intelligent Operations Center ist eine webbasierte Lösung unter Verwendung der Portaltechnologie. Sie können mit einem beliebigen unterstützten Web-Browser auf die Lösung zugreifen.

Informationen zu unterstützten Web-Browsern erhalten Sie über den Link am Ende des Themas.

Zugehörige Informationen:

 Unterstützte Browser für IBM Intelligent Operations Center

Anmelden

Der Zugriff auf die IBM Intelligent Operations Center-Benutzerschnittstelle erfolgt über die Anmeldung.

Vorbereitende Schritte

Benutzer-ID und Kennwort erhalten Sie von Ihrem lokalen Administrator. Er muss sicherstellen, dass Sie über die entsprechende Sicherheitszugriffsebene verfügen, die für Ihre Rolle in der Einrichtung erforderlich ist. Ihr Administrator stellt Ihnen auch die Webadresse (URL) zur Verfügung, über die Sie auf das Lösungsportal zugreifen können.

Informationen zu diesem Vorgang

Im Folgenden wird beschrieben, wie Sie eine neue Browsersitzung starten und IBM Intelligent Operations Center aufrufen. Sie können auf die Lösung auch über andere, in Ihrer Umgebung installierte IBM Smarter Cities Software Solutions zugreifen. Wählen Sie in der Hauptnavigationsleiste oben im Portal **Intelligent Operations Center** aus.

Vorgehensweise

1. Geben Sie die URL in das Adressfeld des Browsers ein.

   Anmerkung: In der URL ist der vollständig qualifizierte Domänenname erforderlich, wie z. B. `http://Hostname_des_Anwendugnsservers/wpsv70/wps/myportal`. Wenn Sie statt der registrierten, vollständig qualifizierten Domäne die IP-Adresse verwenden, werden manche Portlets nicht ordnungsgemäß angezeigt.
2. Geben Sie auf der Anmeldeseite Ihre Benutzer-ID und Ihr Kennwort ein.
3. Klicken Sie auf **Anmelden**.

Ergebnisse

Es werden nur die Seiten, Funktionen und Daten angezeigt, für die Sie eine Zugriffsberechtigung haben. Wenden Sie sich an Ihren Administrator, wenn Sie erweiterte Zugriffsrechte benötigen.

Zugehörige Tasks:

„Abmelden"
Um die IBM Intelligent Operations Center-Benutzerschnittstelle zu schließen und die Serversitzung zu beenden, müssen Sie sich abmelden. Standardmäßig finden Sie den Link für die Abmeldung oben rechts in IBM Intelligent Operations Center.

Abmelden

Um die IBM Intelligent Operations Center-Benutzerschnittstelle zu schließen und die Serversitzung zu beenden, müssen Sie sich abmelden. Standardmäßig finden Sie den Link für die Abmeldung oben rechts in IBM Intelligent Operations Center.

Zugehörige Tasks:

„Anmelden" auf Seite 279
Der Zugriff auf die IBM Intelligent Operations Center-Benutzerschnittstelle erfolgt über die Anmeldung.

Benutzerprofil anzeigen oder bearbeiten

Sie können die Informationen in Ihrem Benutzerprofil für IBM Intelligent Operations Center anzeigen und ändern.

Informationen zu diesem Vorgang

Ihr Profil enthält Informationen, die von Ihnen selbst oder von Ihrem Administrator eingegeben wurden. Sie können Ihr Profil aktualisieren, indem Sie die Informationen in den Attributfeldern ändern (so können Sie beispielsweise ein neues Kennwort festlegen).

Tabelle 81. Benutzerprofilattribute für IBM Intelligent Operations Center

Attribut	Beschreibung	Editierbar durch Benutzer?
User ID* (Benutzer-ID)	Jedem neuen Benutzer wird zu Identifikationszwecken vom Administrator eine ID zugeordnet.	Nein
Password* (Kennwort)	Kennwörter werden vom Administrator aus Sicherheitsgründen zugeordnet. Das Kennwort muss eindeutig sein und eine Länge von 5 bis 60 Zeichen haben. Gültige Kennwörter dürfen nur die Buchstaben a-z, A-Z sowie Punkte ".", Gedankenstriche "-" und Unterstriche "_ " enthalten.	Ja
First Name (Vorname)	Der Vorname kann vom Administrator oder vom Benutzer selbst eingegeben werden.	Ja
Last Name* (Nachname)	Der Nachname wird vom Administrator eingegeben.	Ja
Email (E-Mail)	Die E-Mail-Adresse kann vom Administrator oder vom Benutzer selbst eingegeben werden.	Ja

Anmerkung: Die mit einem Stern (*) markierten Attribute müssen angegeben werden, damit ein neuer Benutzer erstellt werden kann. Die Angabe der nicht markierten Attribute ist optional.

Vorgehensweise

1. Wählen Sie rechts in der Navigationsleiste oben die Option zur Bearbeitung des eigenen Profils aus. Die Attribute Ihres Profils werden angezeigt.
2. So ändern Sie Ihr Kennwort:
   a. Geben Sie Ihr aktuelles Kennwort ein (die Kennwortzeichenfolge wird nicht angezeigt).

b. Geben Sie das neue Kennwort in den Feldern zur Eingabe und zur Bestätigung des Kennworts ein.

3. Bei Bedarf können Sie in den anderen Feldern Informationen eingeben bzw. ändern.
4. Klicken Sie auf **OK**, um die Änderungen zu übergeben.

Ergebnisse

Ihr Benutzerprofil wird entsprechend den Änderungen aktualisiert.

Verwendung von Seiten

Eine Seite besteht aus einem oder mehreren Portlets, die sich gegenseitig ergänzen. In IBM Intelligent Operations Center können Sie mit den Portlets auf einer Seite interagieren und so die erforderlichen Informationen erhalten, um angemessen auf Ereignisse reagieren zu können.

In IBM Intelligent Operations Center sind sechs verschiedene Beispielseitenansichten bereitgestellt.

Wenn Sie über Administratorzugriff verfügen, können Sie in der Seitenansicht auf den Portalservice für die Verwaltung von Seiten zugreifen. Sie können eine Seite bearbeiten oder eine neue Seite erstellen. Klicken Sie auf die rechte Seite der Registerkarte mit dem Seitennamen und wählen Sie im Seitenmenü eine Option aus. Weitere Informationen finden Sie über den Link am Ende des Themas.

Zugehörige Tasks:

„Seite erstellen oder anpassen" auf Seite 153
Sie können neue Seiten erstellen, die im IBM Intelligent Operations Center einbezogen werden sollen, und angeben, welche Portlets auf diesen Seiten angezeigt werden. Sie können die Anzeigengestaltung und das Layout der Portlets auf jeder Seite anpassen.

Ansicht "Aufsichtsperson: Status"

Die Ansicht "Aufsichtsperson: Status" enthält eine konsolidierte Übersicht der KPIs (Key Performance Indicators) und wichtigen Ereignisse. Über die Ansicht "Aufsichtsperson: Status" können Benutzer mit einrichtungsübergreifenden Zuständigkeiten leistungs- und betriebsspezifische Statusänderungen in den Schlüsselbereichen überwachen und verwalten und entsprechende Maßnahmen ergreifen.

Die Ansicht "Aufsichtsperson: Status" ist eine interaktive Webseite. Die Seite enthält die in Tabelle 82 aufgelisteten Portlets. Portlets können als unabhängige Abschnitte dieser Seite gesehen werden, die miteinander kooperieren und damit umfassende Informationen und Interaktionsmöglichkeiten auf Führungsebene bereitstellen.

Tabelle 82. Portlets in der Ansicht "Aufsichtsperson: Status"

Portlet	Beschreibung
„Status" auf Seite 306	Das Portlet "Status" stellt eine für Entscheidungsträger hilfreiche Statusübersicht der KPIs aller Einrichtungen bereit, für die eine Anzeigeberechtigung erteilt wurde. In diesem Portlet können Sie aktuelle Änderungen am KPI-Status anzeigen und damit planen und bei Bedarf entsprechende Maßnahmen vornehmen.

Tabelle 82. Portlets in der Ansicht "Aufsichtsperson: Status" (Forts.)

Portlet	Beschreibung
„Key Performance Indicator - Drilldown” auf Seite 290	Soll eine bestimmte KPI-Kategorie im Portlet "Key Performance Indicator - Drilldown" näher betrachtet werden, klicken Sie im Portlet "Status" auf die Kategorie. Die Kategorie wird daraufhin im Portlet "Key Performance Indicator - Drilldown" angezeigt. In der Liste können Sie die untergeordneten KPIs überprüfen, bis Sie zu den Details des KPI gelangen, der die Statusänderung bewirkt hat.
„Benachrichtigungen” auf Seite 302	Das Portlet "Benachrichtigungen" stellt eine dynamische, interaktive Liste der Alerts bereit, die aufgrund geänderter KPI-Werte und damit in Zusammenhang stehender Ereignisse ausgegeben werden. Dieses Portlet hat die Aufgabe, auf Änderungen von KPI-Werten oder des Ereignisstatus hinzuweisen. Die Liste enthält wichtige Angaben zu jedem Alert.Wenn beispielsweise der Status eines KPI von gelb zu rot wechselt, wird an das Portlet "Benachrichtigungen" ein Alert gesendet.
„Meine Aktivitäten” auf Seite 300	Angemeldete Benutzer können die ihnen zugeordneten Aktivitäten im Portlet "Meine Aktivitäten" anzeigen. Im Portlet "Meine Aktivitäten" sind die Aktivitäten nach übergeordneten SOPs (Standard Operating Procedures) angeordnet. Jede Standard Operating Procedure entspricht einem Ereignis.
„Kontakt” auf Seite 286	Im Portlet "Kontakt" können Ihre Kontakte (Ansprechpartner) nach bestimmten Kategorien angezeigt werden. Sie können die Anordnung nach Personen vornehmen, mit denen Sie kommunizieren müssen. Sie können beispielsweise eine Kategorie für allgemeine Tätigkeiten und eine weitere Kategorie für projektspezifische Tätigkeiten besitzen. Mit dem Portlet "Kontakt" können Sie mit Personen kommunizieren sowie Ihren Onlinestatus, Ihre Ansprechpartner oder Gruppen ändern.

Ansicht "Aufsichtsperson: Vorgänge"

In der Ansicht "Aufsichtsperson: Vorgänge" erhalten Sie eine Übersicht über das Auftreten von Ereignissen. Die Ansicht "Aufsichtsperson: Vorgänge" ist für Aufsichtspersonen und Führungskräfte gedacht, die aktuelle Ereignisse überwachen und für die Planung in Hinsicht auf künftige Ereignisse verantwortlich sind.

Die Ansicht "Aufsichtsperson: Vorgänge" ist eine interaktive Webseite. Die Seite enthält die in Tabelle 83 auf Seite 283 aufgelisteten Portlets. Portlets können als unabhängige Abschnitte dieser Seite gesehen werden, die miteinander kooperieren und damit umfassende Informationen und Interaktionsmöglichkeiten auf Leitungsebene bereitstellen.

Tabelle 83. Portlets in der Ansicht "Aufsichtsperson: Vorgänge"

Portlet	Beschreibung
„Karte" auf Seite 294	Eine Karte der geografischen Region mit Ereignis- und Ressourcenmarkierungen. Ein Filterformular für die Auswahl der Ereigniskategorien, die in der Karte und in den mit dem Portlet "Karte" verknüpften Portlets angezeigt werden sollen. Ein Filterformular für die Auswahl der Funktionen der Ressourcen, die auf der Karte und auf der Registerkarte **Ressourcen** im verknüpften Portlet "Details" angezeigt werden sollen. Um dieses Formular anzuzeigen, wählen Sie zunächst im Portlet "Details" die Option **Ressourcen in der Nähe anzeigen** aus.
„Details" auf Seite 287	"Details" ist ein interaktives Listenportlet. Alle Ereignisse, zu deren Anzeige Sie berechtigt sind, sind in der Ereignisliste sowie in allen Kartenportlets enthalten, die mit dem Portlet "Details" verknüpft sind.
„Benachrichtigungen" auf Seite 302	Das Portlet "Benachrichtigungen" stellt eine dynamische, interaktive Liste der Alerts bereit, die aufgrund geänderter KPI-Werte und damit in Zusammenhang stehender Ereignisse ausgegeben werden. Dieses Portlet hat die Aufgabe, auf Änderungen von KPI-Werten oder des Ereignisstatus hinzuweisen. Die Liste enthält wichtige Angaben zu jedem Alert. Wenn es beispielsweise in einem bestimmten Bereich zu einem Vorfall kommt, wird an das Portlet "Benachrichtigungen" ein Alert gesendet.
„Meine Aktivitäten" auf Seite 300	Angemeldete Benutzer können die ihnen zugeordneten Aktivitäten im Portlet "Meine Aktivitäten" anzeigen. Im Portlet "Meine Aktivitäten" sind die Aktivitäten nach übergeordneten SOPs (Standard Operating Procedures) angeordnet. Jede Standard Operating Procedure entspricht einem Ereignis.
„Kontakt" auf Seite 286	Im Portlet "Kontakt" können Ihre Kontakte (Ansprechpartner) nach bestimmten Kategorien angezeigt werden. Sie können die Anordnung nach Personen vornehmen, mit denen Sie kommunizieren müssen. Sie können beispielsweise eine Kategorie für allgemeine Tätigkeiten und eine weitere Kategorie für projektspezifische Tätigkeiten besitzen. Mit dem Portlet "Kontakt" können Sie mit Personen kommunizieren sowie Ihren Onlinestatus, Ihre Ansprechpartner oder Gruppen ändern.

Ansicht "Betreiber: Vorgänge"

Über die Ansicht "Betreiber: Vorgänge" erhalten Sie einen Überblick über alle Ereignisse und ihre Position. Die Ansicht "Betreiber: Vorgänge" ist für Bediener, Führungskräfte usw. gedacht, die aktuelle Ereignisse überwachen und entsprechende Maßnahmen ergreifen.

Die Ansicht "Betreiber: Vorgänge" ist eine interaktive Webseite. Die Seite enthält die in Tabelle 84 auf Seite 284 aufgelisteten Portlets. Portlets können als unabhängige Abschnitte dieser Seite gesehen werden, die miteinander kooperieren und damit umfassende Informationen und Interaktionsmöglichkeiten auf Betriebsebene bereitstellen.

Tabelle 84. Portlets in der Ansicht "Betreiber: Vorgänge"

Portlet	Beschreibung
„Karte" auf Seite 294	Eine Karte der geografischen Region mit Ereignis- und Ressourcenmarkierungen. Ein Filterformular für die Auswahl der Ereigniskategorien, die in der Karte und in den mit dem Portlet "Karte" verknüpften Portlets angezeigt werden sollen. Ein Filterformular für die Auswahl der Funktionen der Ressourcen, die auf der Karte und auf der Registerkarte **Ressourcen** im verknüpften Portlet "Details" angezeigt werden sollen. Um dieses Formular anzuzeigen, wählen Sie zunächst im Portlet "Details" die Option **Ressourcen in der Nähe anzeigen** aus.
„Details" auf Seite 287	"Details" ist ein interaktives Listenportlet. Alle Ereignisse, zu deren Anzeige Sie berechtigt sind, sind in der Ereignisliste sowie in allen Kartenportlets enthalten, die mit dem Portlet "Details" verknüpft sind.
„Benachrichtigungen" auf Seite 302	Das Portlet "Benachrichtigungen" stellt eine dynamische, interaktive Liste der Alerts bereit, die aufgrund geänderter KPI-Werte und damit in Zusammenhang stehender Ereignisse ausgegeben werden. Dieses Portlet hat die Aufgabe, auf Änderungen von KPI-Werten oder des Ereignisstatus hinzuweisen. Die Liste enthält wichtige Angaben zu jedem Alert. Wenn beispielsweise zwei schwerwiegende Ereignisse an ungefähr derselben Position und nahezu zeitgleich auftreten, wird an das Portlet "Benachrichtigungen" ein Alert gesendet.
„Meine Aktivitäten" auf Seite 300	Angemeldete Benutzer können die ihnen zugeordneten Aktivitäten im Portlet "Meine Aktivitäten" anzeigen. Im Portlet "Meine Aktivitäten" sind die Aktivitäten nach übergeordneten SOPs (Standard Operating Procedures) angeordnet. Jede Standard Operating Procedure entspricht einem Ereignis.
„Kontakt" auf Seite 286	Im Portlet "Kontakt" können Ihre Kontakte (Ansprechpartner) nach bestimmten Kategorien angezeigt werden. Sie können die Anordnung nach Personen vornehmen, mit denen Sie kommunizieren müssen. Sie können beispielsweise eine Kategorie für allgemeine Tätigkeiten und eine weitere Kategorie für projektspezifische Tätigkeiten besitzen. Mit dem Portlet "Kontakt" können Sie mit Personen kommunizieren sowie Ihren Onlinestatus, Ihre Ansprechpartner oder Gruppen ändern.

Aufsichtsperson: Berichte

In der Ansicht "Aufsichtsperson: Berichte" erhalten Sie eine Übersicht über Ereignisdaten, die bei der Ausführung vordefinierter Berichte generiert werden. Außerdem können mithilfe der Ansicht "Aufsichtsperson: Berichte" personalisierte Berichte erstellt und vordefinierte Berichte konfiguriert werden. Diese Berichte sind für Bediener, Führungskräfte usw. gedacht, die aktuelle Ereignisse überwachen und für die Planung im Hinblick auf künftige Ereignisse zuständig sind.

Die Ansicht "Aufsichtsperson: Berichte" ist eine interaktive Webseite, die verschiedene Berichte basierend auf den ausgewählten Daten enthält und Ihnen umfassende Informationen bereitstellt und Interaktionsmöglichkeit auf der Ebene einer Aufsichtsperson bietet. Diese Informationen werden in Diagrammen angezeigt, in denen die Ereignisdaten im System zusammengefasst werden.

In der Ansicht "Aufsichtsperson: Berichte" können Sie die Berichte in „Berichte" auf Seite 304-Portlets konfigurieren und anzeigen. Standardmäßig werden von einigen Berichte-Portlets Beispielberichte angezeigt.

Betreiber: Berichte

Über die Ansicht "Betreiber: Berichte" erhalten Sie eine Übersicht über Berichte, Ereignisse und Alerts. Die Ansicht "Betreiber: Berichte" ist für Bediener, Führungskräfte usw. gedacht, die Berichte überwachen.

In der Ansicht "Betreiber: Berichte" erhalten Sie eine Übersicht über Ereignisdaten, die bei der Ausführung vordefinierter Berichte generiert werden. Darüber hinaus können Sie in der Ansicht "Betreiber: Berichte" personalisierte Berichte anzeigen. Diese Berichte unterstützen Sie bei der Überwachung aktueller Ereignisse, bei Maßnahmen zur Behandlung von Ereignissen und bei der Planung von künftigen Ereignissen.

Die Ansicht "Betreiber: Berichte" ist eine interaktive Webseite. Sie können verschiedene Berichte anzeigen, die Ihnen umfassende Informationen bereitstellen und Interaktionsmöglichkeiten auf Bedienerebene bieten.

In der Ansicht "Betreiber: Berichte" können Sie die Berichte in „Berichte” auf Seite 304-Portlets konfigurieren und anzeigen. Standardmäßig werden von einigen Berichte-Portlets Beispielberichte angezeigt.

Ansicht "Positionskarte"

Über die Ansicht "Positionskarte" erhalten Sie mithilfe einer Positionskarte einen Überblick über alle Ereignisse und ihre Position. Die Ansicht "Positionskarte" ist für Bediener, Führungskräfte usw. gedacht, die aktuelle Ereignisse überwachen und entsprechende Maßnahmen ergreifen.

Die Ansicht "Positionskarte" ist eine interaktive Webseite. Die Seite enthält die in Tabelle 85 aufgelisteten Portlets. Portlets können als unabhängige Abschnitte dieser Seite gesehen werden, die miteinander kooperieren und damit umfassende Informationen und Interaktionsmöglichkeiten auf Betriebsebene bereitstellen.

Tabelle 85. Portlets in der Ansicht "Positionskarte"

Portlet	Beschreibung
„Positionskarte” auf Seite 291	Ein Diagramm der Position mit Markierungen für Ereignisse. Ein Filterformular für die Auswahl der Ereigniskategorien, die in der Karte angezeigt werden sollen. Eine Liste der verfügbaren Positionskarten, angeordnet nach Klassifikation.
„Details” auf Seite 287	"Details" ist ein interaktives Listenportlet. Alle Ereignisse, zu deren Anzeige Sie berechtigt sind, sind in der Ereignisliste sowie in allen Kartenportlets enthalten, die mit dem Portlet "Details" verknüpft sind.

Verwendung von Portlets

Portlets ermöglichen den Zugriff auf Informationen, die auf einer Portalseite angezeigt werden können und mit denen eine Interaktion möglich ist.

In IBM Intelligent Operations Center sind mehrere Portlets enthalten.

Klicken Sie im Portlet in die rechte obere Ecke und wählen Sie aus dem angezeigten Menü **Hilfe** aus, um das Hilfemenü in dem jeweiligen Portlet aufzurufen.

Um die Größe eines Portlets zu ändern, klicken Sie in die obere rechte Ecke des Portlets und wählen Sie die Optionen wie folgt aus dem angezeigten Menü aus:

- Klicken Sie auf die Option zum Maximieren, um das Portlet auf die gesamte Ansicht zu vergrößern.
- Klicken Sie auf die Option zum Minimieren, um den Portletinhalt bis auf die Titelleiste auszublenden.
- Klicken Sie auf die Option zum Wiederherstellen, um die Standardansicht für ein vergrößertes oder ausgeblendetes Portlet wiederherzustellen.

Administrator

Portlet anpassen

Als Administrator können Sie die Einstellungen eines Portlets ändern, indem Sie in die rechte obere Ecke des Portlets klicken und im Portletmenü die gewünschte Option auswählen.

Sie haben zwei Möglichkeiten zur Anpassung; bei beiden Methoden werden die Portleteinstellungen für alle Benutzer geändert:

- **Edit Shared Settings** (Gemeinsam genutzte Einstellungen bearbeiten): Über diese Option werden nur die Einstellungen für die aktuelle Portletinstanz geändert.
- **Configure** (Konfigurieren): Über diese Option werden die globalen Portleteinstellungen für alle vorhandenen Portletinstanzen geändert.

Welche Anpassungsmöglichkeiten Sie haben, hängt von den Berechtigungen ab, die Ihrer Benutzer-ID zugeordnet sind. Globale Einstellungen werden durch gemeinsam genutzte Einstellungen außer Kraft gesetzt.

Einige Einstellungen der in IBM Intelligent Operations Center bereitgestellten Portlets sind vom Portlettyp abhängig (beispielsweise die Standardzoomstufe für eine Karte). Darüber hinaus können Sie noch generische Portletparameter setzen, die für alle bereitgestellten Portlets gelten (beispielsweise den Portlet-Titel).

Kontakt

Mithilfe des Portlets "Kontakt" können Sie Sofortnachrichten innerhalb der Lösung senden.

Im Portlet "Kontakt" können Ihre Kontakte (Ansprechpartner) nach bestimmten Kategorien angezeigt werden. Sie können die Anordnung nach Personen vornehmen, mit denen Sie kommunizieren müssen. Sie können beispielsweise eine Kategorie für allgemeine Tätigkeiten und eine weitere Kategorie für projektspezifische Tätigkeiten besitzen. Mit dem Portlet "Kontakt" können Sie mit Personen kommunizieren sowie Ihren Onlinestatus, Ihre Ansprechpartner oder Gruppen ändern.

Klicken Sie oben im Portlet auf die Menüs:

- **Datei**: Über dieses Menü können Sie Ansprechpartner hinzufügen, Gruppen ändern oder sich abmelden.
- **Tools**: Über dieses Menü können Sie einen Chat, eine Besprechung oder eine Ankündigung konfigurieren und außerdem Ihre Datenschutzeinstellungen ändern.
- **Hilfe**: Über dieses Menü können Sie ausführliche Informationen zur Verwendung des Portlets abrufen.

Klicken Sie auf Ihren Status, um Ihren Status und die Nachricht zu ändern. Der Standardstatus gibt an, dass Sie verfügbar sind. Durch die entsprechende Änderung Ihres Status können Sie angeben, dass Sie nicht am Platz sind, sich in einer Besprechung befinden oder nicht gestört werden möchten.

Der Status von angemeldeten Benutzern wird im Portlet "Kontakt" angezeigt. Wenn ein angemeldeter Benutzer das Browserfenster schließt oder sich bei WebSphere Portal abmeldet, wird der Status dieses Benutzers weiterhin als angemeldet angezeigt, bis die Sitzung abläuft. Alle Nachrichten, die an diesen Benutzer gesendet werden, nachdem der Benutzer das Browserfenster geschlossen oder sich abgemeldet hat, werden nicht zugestellt. Demzufolge wird dem Benutzer, der versucht, die Nachricht zu senden, eine Fehlernachricht angezeigt. Um sicherzustellen, dass Ihr Status sofort aktualisiert wird, klicken Sie zum Abmelden im Portlet "Kontakt" auf **Datei** > **Abmelden**.

Anmerkung: Damit dieses Portlet wie erwartet funktioniert, müssen Sie sich am Lösungsportal mit dem vollständig qualifizierten Domänennamen des IBM Intelligent Operations Center-Anwendungsservers anmelden. Wenn Sie sich mit einer IP-Adresse oder einem Hostnamenalias anstatt mit dem registrierten, vollständig qualifizierten Domänennamen am Portal anmelden, wird dieses Portlet nicht ordnungsgemäß angezeigt.

Administrator

Wenn Sie Administratorzugriff besitzen, können Sie dieses Portlet anpassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Folgende Einstellungen für das Portlet "Kontakt" können geändert werden:

- Hilfedatei
- Portlethöhe
- Portlethöhe bei Vollbild
- Portlet-Titel
- Ressourcenpaket

Zugehörige Verweise:

„Einstellungen des Kontakt-Portlets" auf Seite 155
Anpassen des Kontakt-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Details

Mit dem Portlet "Details" können Sie in IBM Intelligent Operations Center Ereignisse anzeigen, überwachen und verwalten.

"Details" ist ein interaktives Listenportlet. Alle Ereignisse, zu deren Anzeige Sie berechtigt sind, sind in der Ereignisliste sowie in allen Kartenportlets enthalten, die mit dem Portlet "Details" verknüpft sind.

Die Ressourcen in der Nähe eines Ereignisses können in einer Ressourcenliste und in einer Karte angezeigt werden.

Ereignisse und Ressourcen

Das Portlet "Details" enthält die beiden in der folgenden Tabelle aufgeführten interaktiven Schnittstellenelemente:

Tabelle 86. Portlet "Details" - Anzeige

Schnittstellenelement	Beschreibung
Ereignisse und Vorfälle	Die Ereignisliste enthält wichtige Details zu den einzelnen Ereignissen. Eine ausführlichere Beschreibung der Ereignisse wird angezeigt, wenn Sie den Cursor über die entsprechende Zeile in der Liste bewegen.
Ressourcen	Wenn Sie mit der rechten Maustaste auf ein Ereignis klicken, werden wichtige Details zu den Ressourcen in der Nähe des betreffenden Ereignisses aufgelistet. Eine ausführlichere Beschreibung einer Ressource wird angezeigt, wenn Sie den Cursor über die Zeile in der Liste bewegen.

Wenn Sie IBM Intelligent Operations Center öffnen, werden im Portlet "Details" zunächst alle für Sie relevanten Ereignisse angezeigt.

Im Portlet "Karte" können Sie die Ereigniskategorien und Ressourcenfunktionen auswählen, die angezeigt werden sollen. Auf der Registerkarte **Ereignisse und Vorfälle** werden dieselben Ereigniskategorien wie im Portlet "Karte" angezeigt. Auch die auf der Registerkarte **Ressourcen** angezeigten Funktionen von Ressourcen sind dieselben wie im Portlet "Karte".

Die Ereignisliste wird (in Abhängigkeit von den von Ihnen festgelegten Filtern, mit denen die Anzahl der angezeigten Kategorien eingeschränkt wird) beim Auftreten neuer Ereignisse und bei Änderungen aktualisiert.

Ein Zähler in der linken Ecke der Aktionsleiste am Ende der Liste gibt die Anzahl der Elemente, die angezeigt werden, sowie die Anzahl der Elemente insgesamt an. In der Mitte der Aktionsleiste können Sie die Anzahl der Elemente auswählen, die gleichzeitig angezeigt werden sollen. Sind mehr Zeilen vorhanden, als gleichzeitig angezeigt werden können, können Sie die Seite über die Schaltflächen in der rechten Ecke der Aktionsleiste nach oben bzw. nach unten verschieben.

Ereigniseigenschaften

In der folgenden Tabelle sind die Eigenschaften aufgeführt, die der Beschreibung eines Ereignisses dienen:

Tabelle 87. Ereigniseigenschaften

Eigenschaft	**Inhalt**
Wer	
Absender	Die Quellen- oder Benutzer-ID.
Name des Ansprechpartners	Name des Ansprechpartners für weitere Informationen.
E-Mail des Ansprechpartners	E-Mail-Adresse des Ansprechpartners.
Rufnummer des Ansprechpartners	Die Telefonnummer des Ansprechpartners.
Was	
Ereignistyp*	Gibt den Ereignistyp innerhalb von *Kategorie* an.
Ereignisstatus*	Hinweise zur Behandlung von Ereignissen.
Ereignisverbreitung*	Zielgruppe, an die die Nachricht gesendet wird.
Einschränkung	Zusätzlich erforderliche Informationen, wenn "Eingeschränkt" für *Ereignisverbreitung* angegeben ist.
Kurzbeschreibung*	Eine kurze Beschreibung des Ereignisses.
Kategorie*	Allgemeine Klassifizierung von Ereignissen
Schweregrad*	Gibt den Grad der Auswirkung des Ereignisses an.
Gewissheit*	Gibt die Verlässlichkeit der Ereignisvorhersage an.
Dringlichkeit*	Zeitrahmen für die Reaktion auf das Ereignis.
Nachrichtentyp	Gibt an, um was für eine Nachricht es sich handelt.
Beschreibung	Zusätzliche Beschreibung des Ereignisses.
Webadresse	Webadresse, unter der zusätzliche Informationen zum Ereignis zu finden sind.
Wann	
Sendedatum und -uhrzeit	Gibt an, an welchem Tag und um welche Uhrzeit die Nachricht übergeben bzw. gesendet wurde.
Wirksamkeitsdatum und -uhrzeit	Gibt an, an welchem Tag und um welche Uhrzeit die Nachricht wirksam wird.
Startdatum und - uhrzeit	Gibt an, an welchem Tag und um welche Uhrzeit das Ereignis voraussichtlich beginnt.
Ablaufdatum und -uhrzeit	Gibt an, an welchem Tag und um welche Uhrzeit das Ereignis voraussichtlich endet.
Wo	
Beschreibung des Bereichs	Beschreibung des betroffenen Bereichs.

Tabelle 87. Ereigniseigenschaften (Forts.)

Eigenschaft	Inhalt
Wer	
Breitengrad und Längengrad	Koordinaten der Position des Ereignisses.

Anmerkung: Die in der Tabelle mit einem Stern (*) markierten Eigenschaften müssen angegeben werden, damit ein neues Ereignis erstellt werden kann. Die Angabe der nicht markierten Eigenschaften ist bei der Erstellung eines Ereignisses optional.

Ereignisse und Vorfälle verwalten

Sie können im Portlet "Details" eine Reihe von Aktionen für die auf der Registerkarte **Ereignisse und Vorfälle** aufgeführten Ereignisse ausführen. Im Portlet "Karte" können Sie Ereignisse hinzufügen, die sowohl auf der Karte als auch in der Ereignisliste des Portlets "Details" angezeigt werden.

Vorgehensweise

Klicken Sie auf der Registerkarte **Ereignisse und Vorfälle** mit der rechten Maustaste auf eine Zeile in der Ereignisliste und wählen Sie in dem angezeigten Menü die gewünschte Option aus:

- Sollen die Informationen zu einem Ereignis aktualisiert werden, klicken Sie auf **Ereignis aktualisieren**. Sie können die Änderungen in einem Fenster mit Feldern eingeben, die Informationen zu dem Ereignis enthalten. Wenn ein Ereignisdatensatz geändert wird, wird die Eigenschaft "Nachrichtentyp" in *Aktualisieren* geändert.
- Soll ein Ereignisstatus in "Vorfall" geändert werden, klicken Sie auf **Zu Vorfall eskalieren**, um ein Fenster zu öffnen, in dem Sie Ihre Kontaktinformationen eingeben können. Bei der Eskalation eines Ereignisdatensatzes ändern sich die Eigenschaften und das Symbol auf der Karte.
- Soll ein Ereignis aus der Liste und aus der Karte entfernt werden, klicken Sie auf **Ereignis abbrechen**, um ein Fenster zu öffnen, in dem Sie Ihre Kontaktinformationen eingeben können.
- Sollen die einem Ereignis zugeordneten Aktivitäten der SOP (Standard Operating Procedure) und die zugeordneten Workflowaktivitäten angezeigt werden, klicken Sie auf **View Standard Operating Procedure Details** (Details der Standard Operating Procedure anzeigen). Sind einem Ereignis keine SOPs (Standard Operating Procedures) zugeordnet, steht diese Option nicht zur Auswahl. Ist eine Standard Operating Procedure zugeordnet, wird sie im Fenster **SOP-Details** angezeigt. Die einer Standard Operating Procedure zugeordneten Workflowaktivitäten können über das Portlet "Meine Aktivitäten" verwaltet werden.
- Soll eine Liste der Ressourcen im näheren Umfeld eines Ereignisses angezeigt werden, klicken Sie auf **Ressourcen in der Nähe anzeigen** und wählen Sie den Radius des gewünschten Bereichs aus. Auf der Registerkarte **Ressourcen** wird eine Liste mit Ressourcen angezeigt.
- Sollen Informationen zu einem Ereignis angezeigt werden, klicken Sie auf **Eigenschaften**, um ein Fenster mit Feldern zu öffnen, die Informationen zum Ereignis enthalten.

Ressourcen verwalten

Sie können für die auf der Registerkarte **Ressourcen** aufgelisteten Ressourcen eine Reihe von Aktionen ausführen.

Vorgehensweise

Klicken Sie auf der Registerkarte **Ressourcen** mit der rechten Maustaste auf eine Zeile in der Ressourcenliste und wählen Sie in dem angezeigten Menü die gewünschte Option aus:

- Sollen die Informationen zu einer Ressource aktualisiert werden, klicken Sie auf **Aktualisieren**.
- Soll eine Ressource aus der Liste und aus der Karte entfernt werden, klicken Sie auf **Löschen**.
- Sollen Informationen zu einer Ressource angezeigt werden, klicken Sie auf **Eigenschaften**.

Die Ressource wird (unabhängig von der von Ihnen gewählten Option) in Tivoli Service Request Manager auf der Registerkarte **Ressourcen** angezeigt. Darüber hinaus können Sie auf der Registerkarte Tivoli Service Request Manager **Funktionen** die Funktionen der Ressource anzeigen. Soll eine Ressource aktualisiert oder gelöscht werden, wählen Sie die betreffende Ressource aus und wählen Sie anschließend in der Liste **Select Action** (Aktion auswählen) die gewünschte Option aus.

Portlet "Details" anpassen

Administrator

Wenn Sie Administratorzugriff besitzen, können Sie dieses Portlet anpassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Setzen Sie die Parameter für das Portlet "Details" wie folgt:

Über die Parameter für das Portlet "Details" können Sie folgende Einstellungen vornehmen:

- Geben Sie Spaltenanordnung, Überschriften, Sortierreihenfolge und Priorität an.
- Geben Sie zusätzliche Filterbedingungen für die Anzeige von Ereignissen und Ressourcen an.
- Blenden Sie folgende Elemente ein bzw. aus:
  - Schaltfläche **Ereignis hinzufügen**
  - Schaltfläche **Ressource hinzufügen**
  - Registerkarte **Ereignisse**
  - Registerkarte **Ressourcen**
  - Die Symbolleiste oben in der Liste.
- Geben Sie einen Gruppennamen an, um die Kommunikation mit anderen Kartenportlets und Portlets des Typs "Details" zu ermöglichen.
- Konfigurieren Sie das Portlet so, dass bestimmte Nachrichtentypen von anderen Portlets in der Gruppe akzeptiert bzw. ignoriert werden.

Sie können generische Portletparameter setzen, die für alle Portlets gelten (den Verzeichnispfad der Hilfedatei, die Höhe des Portlets, den Portlet-Titel und das Ressourcenpaket).

Zugehörige Verweise:

„Einstellungen des Details-Portlets” auf Seite 156
Anpassen des Details-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Key Performance Indicator - Drilldown

Mit dem Portlet "Key Performance Indicator - Drilldown" können Sie weitere Informationen zu einer KPI-Kategorie, den Status der untergeordneten KPIs anzeigen.

Im Portlet "Key Performance Indicator - Drilldown" werden alle zugrunde liegenden KPIs angezeigt, die einer im Portlet "Status" angezeigten Einrichtung oder KPI-Kategorie zugeordnet sind. Die KPIs werden in Form einer verschachtelten Liste angezeigt, deren Ebenen ein- oder ausgeblendet werden können. Der Status der einzelnen KPIs wird anhand von Farben angegeben; ebenso werden Farben auch für die im Portlet "Status" angezeigten KPI-Kategorien verwendet. Die Werte der untergeordneten KPIs bestimmen die Farbe des jeweils übergeordneten KPI. Um den Status des KPI anzuzeigen, bewegen Sie den Cursor über den betreffenden KPI.

Soll eine bestimmte KPI-Kategorie im Portlet "Key Performance Indicator - Drilldown" näher betrachtet werden, klicken Sie im Portlet "Status" auf die Kategorie. Die Kategorie wird daraufhin im Portlet "Key

Performance Indicator - Drilldown" angezeigt. In der Liste können Sie die untergeordneten KPIs überprüfen, bis Sie zu den Details des KPI gelangen, der die Statusänderung bewirkt hat.

Administrator

Portlet "Key Performance Indicator - Drilldown" anpassen

Wenn Sie Administratorzugriff besitzen, können Sie dieses Portlet anpassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Über die Parameter für das Portlet "Key Performance Indicator - Drilldown" können Sie folgende Einstellungen vornehmen:

- Geben Sie Spaltenanordnung, Überschriften, Sortierreihenfolge und Priorität an.
- Die Farben für die KPIs anpassen.
- Weitere KPI-Filter aktivieren.
- Blenden Sie die Symbolleiste oben in der Liste ein bzw. blenden Sie sie aus.
- Einen Gruppennamen angeben, um die Kommunikation mit dem Portlet "Key Performance Indicator - Drilldown" zu ermöglichen.

Sie können generische Portletparameter setzen, die für alle Portlets gelten (den Verzeichnispfad der Hilfedatei, die Höhe des Portlets, den Portlet-Titel und das Ressourcenpaket).

Zugehörige Konzepte:

„Key Performance Indicators (KPIs)" auf Seite 178
Mit dem Portlet "Key Performance Indicators (KPIs)" können Sie KPIs (Key Performance Indicator) und ihre hierarchische Anzeige in IBM Intelligent Operations Center anpassen.

Zugehörige Verweise:

„Einstellungen des Key Performance Indicator - Drilldown-Portlets" auf Seite 161
Anpassen des Key Performance Indicator - Drilldown-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Positionskarte

Mit dem Portlet "Positionskarte" können Sie die auf einer Positionskarte markierten Ereignisse anzeigen. Eine Positionskarte im IBM Intelligent Operations Center ist eine Karte oder ein Plan mit vordefinierten Interaktionsbereichen, wie z. B. Sitzbereiche in großen Sportstadien.

Im Portlet "Positionskarte" werden Ereignisse grafisch an den Positionen angezeigt, an denen sie auftreten. Mithilfe der drei Portlets "Positionskarte", "Karte" und "Details" können Sie Probleme, Positionsmuster, Konflikte und Synergieeffekte ermitteln.

Die Portlets "Positionskarte", "Karte" und "Details" können miteinander verknüpft werden, sodass sie Eingaben sowie Änderungen an den angezeigten Ereignissen gemeinsam nutzen können. Im Portlet "Positionskarte" können Sie die Ereigniskategorien auswählen, die angezeigt werden sollen. Durch die Auswahl der Kategorien werden die Ereignisse vorgegeben, die im Portlet "Positionskarte" sowie in den mit ihm verknüpften Portlets "Karte" und "Details" angezeigt werden.

Positionskarte - Schnittstelle

Das Portlet "Positionskarte" enthält die drei in der folgenden Tabelle aufgeführten interaktiven Schnittstellenelemente:

Tabelle 88. Schnittstellenelemente des Portlets "Positionskarte"

Schnittstellenelement	Beschreibung
Positionskarte	Ein Diagramm der Position mit Markierungen für Ereignisse.
Inhalt auswählen: Ereigniskategorien	Ein Filterformular für die Auswahl der Ereigniskategorien, die in der Karte angezeigt werden sollen.
Kartenmenü	Eine Liste der verfügbaren Positionskarten, angeordnet nach Klassifikation.

Beim Öffnen der Portalseite wird das Portlet "Positionskarte" zunächst mit allen für Sie relevanten Ereignissen auf der Positionskarte angezeigt. Diese Karte wird (in Abhängigkeit von den von Ihnen festgelegten Filtern, mit denen die Anzahl der angezeigten Kategorien eingeschränkt wird) beim Auftreten neuer Ereignisse aktualisiert. Links neben der Karte wird eine Menüleiste mit allen verfügbaren Karten angezeigt.

Beim Auftreten eines Ereignisses in einem Bereich wird auf der Positionskarte an der betreffenden Position eine Markierung gesetzt. Sie können eine Kurzbeschreibung sowie eine Beschreibung des Ereignisses anzeigen, indem Sie den Cursor über die Ereignismarkierung auf der Karte bewegen. Das Fenster enthält Name und Beschreibung des Bereichs, in dem das Ereignis aufgetreten ist. Kommt es in einem Bereich zu mehreren Ereignissen, werden diese zusammengefasst und durch eine Gruppenmarkierung gekennzeichnet. Wenn Sie den Cursor über diese Markierung bewegen, werden im Fenster auch die Kurzüberschriften der Ereignisse angezeigt. Wird der Cursor über vordefinierte Bereiche ohne Ereignisse in der Karte bewegt, werden Name und Beschreibung des Bereichs angezeigt.

Sind Verknüpfungen mit Portlets vorhanden und klicken Sie in diesem Portlet auf ein Ereignis, werden die entsprechenden Ereignisse in den anderen Portlets in der Gruppe ebenfalls ausgewählt. Ebenso wird beim Hervorheben eines Ereignisses in einem der verknüpften Portlets dieses Ereignis auch in diesem Portlet hervorgehoben.

Anmerkung: Damit ein Ereignis im Portlet "Positionskarte" angezeigt wird, muss es über eine Bereichs-ID verfügen. Damit eine Anzeige in den Portlets "Positionskarte" und "Karte" möglich ist, müssen für Ereignisse außerdem Längen- und Breitengrade angegeben sein. Ereignisse ohne Bereichs-ID oder Koordinaten können nur im Portlet "Details" angezeigt werden.

Kartenmarkierungen

Die Position von Ereignissen wird auf der Karte mit einer der folgenden Markierungen angegeben:

Tabelle 89. Kartenmarkierungen

Markierungstyp	Beschreibung
Symbol	Zeigt auf der Karte die genaue Position eines Ereignisses an; für jede Ereigniskategorie ist ein eigenes Symbol vorhanden.
Gruppe	Zeigt an, dass in einem Bereich mehrere Ereignisse aufgetreten sind, und gibt die Anzahl dieser Ereignisse an.

Das Symbol für einen Ereignistyp wird auf der Registerkarte **Ereignisse und Vorfälle** des Portlets "Details" im Kategorienfeld in den Ereignisdetails definiert. Bei der Eskalierung eines Ereignisses zu einem Vorfall wird auf der Karte weiterhin das definierte Kategoriesymbol angezeigt, allerdings mit einem roten Rand um das Symbol herum.

Steuerungselemente für Karten

Sie können mithilfe der Maus oder der Tastatur den Cursor auf der Karte verschieben.

Die Steuerelemente der Karte befinden sich auf der oberen linken Seite der Karte.

Die Steuerelemente der Karte befinden sich oben links auf der Karte. Sie umfassen:
- Schwenkpfeile (oben, unten, links, rechts)
- Vergrößern
- Weltansicht (maximale Verkleinerung)
- Verkleinern

Schwenksteuerung für die Navigation auf der Karte

Sie können folgendermaßen auf der Karte navigieren:
- Klicken Sie und ziehen Sie die Karte mithilfe der Maus
- Drücken Sie auf den oberen Schwenkpfeil oder auf den Aufwärtspfeil auf der Tastatur, um nach Norden zu schwenken
- Drücken Sie auf den unteren Schwenkpfeil oder auf den Abwärtspfeil auf der Tastatur, um nach Süden zu schwenken
- Drücken Sie auf den rechten Schwenkpfeil oder auf den Rechtspfeil auf der Tastatur, um nach Osten zu schwenken
- Drücken Sie auf den linken Schwenkpfeil oder auf den Linkspfeil auf der Tastatur, um nach Westen zu schwenken

Zoomsteuerelemente für das Vergrößern und Verkleinern der Kartenskala

Sie können die Karte folgendermaßen verkleinern und vergrößern:
- Klicken Sie auf das Kartensymbol **+**, um die Kartenmitte zu vergrößern, und auf **-**, um sie zu verkleinern
- Klicken Sie doppelt auf die Maus, um die Karte zu zentrieren und die ausgewählte Position zu vergrößern
- Klicken Sie auf das Symbol für die Weltansicht, um die Ansicht zu minimieren und die Weltansicht darzustellen
- Drücken Sie die Taste **+** auf Ihrer Tastatur, um zu vergrößern
- Drücken Sie die Taste **-** auf Ihrer Tastatur, um zu verkleinern
- Drücken Sie bei der Verwendung der Maus auf die Umschalttaste, um ein Rechteck um den Bereich zu zeichnen und diesen zu vergrößern

Ereigniskategorien für die Karte auswählen

Mithilfe des Filters "Ereigniskategorien" können Sie durch Auswahl der Kategorie vorgeben, welche Ereignisse auf der Karte angezeigt werden sollen.

Klicken Sie auf **Inhalt auswählen**, um das Filterformular anzuzeigen. Über das Filterformular können Sie vorgeben, welche Ereigniskategorien auf der Karte und in den zugehörigen Portlets angezeigt werden sollen. Wenn beispielsweise eine bestimmte Ereigniskategorie für Sie von Interesse ist, die analysiert werden soll, können Sie über diesen Filter alle für Sie nicht relevanten Ereigniskategorien ausblenden. Alle Änderungen im Filterformular werden auf der Karte übernommen. Wird die Auswahl geändert, wird die Karte aktualisiert und es werden nur die Positionen der Ereignisse markiert, die zu den ausgewählten Kategorien gehören. Die Ereigniskategorien, die angezeigt bzw. nicht angezeigt werden sollen, werden über die Kontrollkästchen im Filterformular ausgewählt bzw. abgewählt. Um das Filterformular zu schließen, klicken Sie auf **Inhalt auswählen**. Wenn Sie die Portalseite verlassen und anschließend wieder zurückkehren, wird der Filter wieder auf die Standardauswahl zurückgesetzt.

Sie können einzelne Ereignisse hervorheben, die analysiert werden sollen, indem Sie im Portlet "Details" die entsprechenden Kontrollkästchen auswählen. Die betreffenden Ereignisse werden auch in den verknüpften Portlets hervorgehoben.

Portlet "Positionskarte" anpassen

Administrator

Wenn Sie Administratorzugriff besitzen, können Sie dieses Portlet anpassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Die Portlets "Karte" und "Positionskarte" können ebenfalls über Änderungen an globalen Einstellungen angepasst werden. Über globale Einstellungen wird der Inhalt des Portlets für alle Benutzer und alle Portletinstanzen vorgegeben. Globale Einstellungen werden durch gemeinsam genutzte Einstellungen außer Kraft gesetzt.

Folgende Einstellungen für das Portlet "Positionskarte" können geändert werden:

- Die Standardauswahl des Filters "Ereigniskategorien".
- Der Name der Standardpositionskarte, die angezeigt werden soll.
- Die Standardfarbe zum Hervorheben eines Bereichs, wenn Sie den Cursor über einen Bereich bewegen.
- Der Name der Gruppe, die eine Kommunikation mit anderen Kartenportlets und Details-Portlets ermöglicht.

Sie können generische Portletparameter setzen, die für alle Portlets gelten (den Verzeichnispfad der Hilfedatei, die Höhe des Portlets, den Portlet-Titel und das Ressourcenpaket).

Positionskarten anpassen

Mithilfe des Portlets "Positionskartenmanager" können Sie Folgendes im Portlet "Positionskarte" anpassen:

- Der Klassifikationsname, der im Menü links im Portlet angezeigt werden soll.
- Die Karte, die im Portlet angezeigt werden soll.
- Die Bereiche in einer Karte.

Zugehörige Konzepte:

„Positionskartenmanager" auf Seite 186
Mithilfe des Portlets "Positionskartenmanager" können Sie das Portlet "Positionskarte" anpassen.

Zugehörige Verweise:

„Einstellungen des Positionskarte-Portlets" auf Seite 164
Anpassen des Positionskarte-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Karte

Mit dem Portlet "Karte" können Sie die in einer Karte enthaltenen Ereignisse und Ressourcen anzeigen.

Das Portlet "Karte" enthält eine grafische Darstellung der in einer Karte enthaltenen Ereignisse und Ressourcen. Mithilfe der drei Portlets "Karte", "Positionskarte" und "Details" können Sie Positionsmuster, Konflikte, Probleme und Synergieeffekte ermitteln.

Die Portlets "Karte", "Positionskarte" und "Details" können miteinander verknüpft werden, sodass sie Eingaben sowie Änderungen an den angezeigten Ereignissen gemeinsam nutzen können. Im Portlet "Karte" können Sie die Ereigniskategorien und Ressourcenfunktionen auswählen, die angezeigt werden sollen. Mit Ihrer Auswahl geben Sie vor, was im Portlet "Karte" sowie in den verknüpften Portlets "Positionskarte" und "Details" angezeigt wird.

Portlet "Karte" - Schnittstellen

Das Portlet "Karte" enthält die drei in der folgenden Tabelle aufgeführten interaktiven Schnittstellenelemente:

Tabelle 90. Schnittstellenelemente des Portlets "Karte"

Schnittstellenelement	Beschreibung
Karte	Eine Karte der geografischen Region mit Ereignis- und Ressourcenmarkierungen.
Inhalt auswählen: Ereigniskategorien	Ein Filterformular für die Auswahl der Ereigniskategorien, die in der Karte und in den mit dem Portlet "Karte" verknüpften Portlets angezeigt werden sollen.
Inhalt auswählen: Ressourcen	Ein Filterformular für die Auswahl der Funktionen der Ressourcen, die auf der Karte und auf der Registerkarte **Ressourcen** im verknüpften Portlet "Details" angezeigt werden sollen. Um dieses Formular anzuzeigen, wählen Sie zunächst im Portlet "Details" die Option **Ressourcen in der Nähe anzeigen** aus.

Beim Öffnen der Portalseite wird das Portlet "Karte" zunächst mit allen für Sie relevanten Ereignissen auf der Karte angezeigt. Sind Längen- und Breitengrade für ein Ereignis angegeben, wird die Ereignisposition in Form einer Symbolmarkierung auf der Karte angegeben. Sie können eine Kurzbeschreibung sowie eine Beschreibung des Ereignisses anzeigen, indem Sie den Cursor über die Ereignismarkierung auf der Karte bewegen. Sind an einer Position mehrere Ereignisse vorhanden, wird die Anzahl der Ereignisse auf der Markierung angezeigt. Wenn Sie den Cursor über diese Gruppenmarkierung bewegen, werden im Fenster auch die Überschriften der Ereignisse angezeigt. Diese Karte wird (in Abhängigkeit von den von Ihnen festgelegten Filtern, mit denen die Anzahl der angezeigten Kategorien eingeschränkt wird) beim Auftreten neuer Ereignisse aktualisiert.

Sind Verknüpfungen mit Portlets vorhanden und klicken Sie in einem Portlet auf eine Ereignismarkierung, wird das entsprechende Ereignis in den anderen Portlets in der Gruppe ebenfalls ausgewählt.

Die Anzahl der Markierungen, die auf der Karte angezeigt werden können, ist beschränkt. Die Markierungen, die die Mindestanzahl für den angezeigten Bereich überschreiten, werden nicht angezeigt. In diesem Fall erhalten Sie eine Nachricht mit der Anzahl der verfügbaren Markierungen und der maximal möglichen Anzahl an Markierungen. Sie haben zwei Möglichkeiten, alle verfügbaren Markierungen anzuzeigen:

- Vergrößern Sie einen Bereich der Karte bzw. wechseln Sie zu einem Bereich der Karte, in dem die Anzahl der Markierungen unter dem Grenzwert liegt.
- Klicken Sie auf **Alle Elemente in der Ansicht laden**.

Bei Auswahl der zweiten Option werden die Markierungen langsamer auf der Karte angezeigt. Sie haben noch eine dritte Möglichkeit: Verringern Sie über einen Filter die Anzahl der angezeigten Kategorien.

Bei Auswahl der Option **Ressourcen in der Nähe anzeigen** für ein Ereignis im Portlet "Details" werden die Ressourcen auf Basis des von Ihnen ausgewählten Radius sowie anhand der ausgewählten Funktionen auf der Karte angezeigt.

Die Karte stellt immer eine aktuelle Übersicht bereit, indem neue Ereignisse (in Abhängigkeit von den von Ihnen festgelegten Filtern, mit denen die Anzahl der angezeigten Kategorien eingeschränkt wird) hinzugefügt werden.

Anmerkung: Wurde für ein Ereignis neben Längen- und Breitengraden auch eine Bereichs-ID angegeben, kann es in den Portlets "Positionskarte" und "Karte" angezeigt werden. Im Portlet "Details" können alle Ereignisse angezeigt werden.

Kartenmarkierungen

Die Position von Ereignissen und Ressourcen wird auf der Karte mit einer der folgenden Markierungen angegeben:

Tabelle 91. Kartenmarkierungen

Markierungstyp	Beschreibung
Symbol	Zeigt auf der Karte die genaue Position eines Ereignisses oder einer Ressource an; für jede Ereignis- bzw. Ressourcenkategorie ist ein eigenes Symbol vorhanden.
Polygon	Umreißt auf der Karte den Bereich für ein bestimmtes Ereignis.
Gruppe	Zeigt an, dass an einer Position mehrere Ereignisse aufgetreten sind, und gibt die Anzahl dieser Ereignisse an.
Radius	Umreißt auf der Karte den Bereich, den Sie über **Ressourcen in der Nähe anzeigen** für ein Ereignis ausgewählt haben.

Das Symbol für einen Ereignistyp wird auf der Registerkarte **Ereignisse und Vorfälle** des Portlets "Details" im Kategorienfeld in den Ereignisdetails definiert. Bei der Eskalierung eines Ereignisses zu einem Vorfall wird auf der Karte weiterhin das definierte Kategoriesymbol angezeigt, allerdings mit einem roten Rand. Bei Klicken auf eine Ereignismarkierung wird das zugehörige Ereignis (bzw. die zugehörigen Ereignisse) im Portlet "Details" hervorgehoben.

Das Symbol für eine Ressource wird auf der Registerkarte **Ressourcen** des Portlets "Details" im Typfeld in den Ressourcendetails definiert. Um die Ressourcensymbole anzuzeigen, wählen Sie zunächst im Portlet "Details" die Option **Ressourcen in der Nähe anzeigen** aus.

Verwendung der Steuerelemente für Karten

Sie können mithilfe der Maus oder der Tastatur den Cursor auf der Karte verschieben.

Die Steuerelemente der Karte befinden sich auf der oberen linken Seite der Karte.

Die Steuerelemente der Karte befinden sich oben links auf der Karte. Sie umfassen:

- Schwenkpfeile (oben, unten, links, rechts)
- Vergrößern
- Weltansicht (maximale Verkleinerung)
- Verkleinern

Schwenksteuerung für die Navigation auf der Karte

Sie können folgendermaßen auf der Karte navigieren:

- Klicken Sie und ziehen Sie die Karte mithilfe der Maus
- Drücken Sie auf den oberen Schwenkpfeil oder auf den Aufwärtspfeil auf der Tastatur, um nach Norden zu schwenken
- Drücken Sie auf den unteren Schwenkpfeil oder auf den Abwärtspfeil auf der Tastatur, um nach Süden zu schwenken
- Drücken Sie auf den rechten Schwenkpfeil oder auf den Rechtspfeil auf der Tastatur, um nach Osten zu schwenken
- Drücken Sie auf den linken Schwenkpfeil oder auf den Linkspfeil auf der Tastatur, um nach Westen zu schwenken

Zoomsteuerelemente für das Vergrößern und Verkleinern der Kartenskala

Sie können die Karte folgendermaßen verkleinern und vergrößern:

- Klicken Sie auf das Kartensymbol **+**, um die Kartenmitte zu vergrößern, und auf **-**, um sie zu verkleinern
- Klicken Sie doppelt auf die Maus, um die Karte zu zentrieren und die ausgewählte Position zu vergrößern
- Klicken Sie auf das Symbol für die Weltansicht, um die Ansicht zu minimieren und die Weltansicht darzustellen
- Drücken Sie die Taste **+** auf Ihrer Tastatur, um zu vergrößern
- Drücken Sie die Taste **-** auf Ihrer Tastatur, um zu verkleinern
- Drücken Sie bei der Verwendung der Maus auf die Umschalttaste, um ein Rechteck um den Bereich zu zeichnen und diesen zu vergrößern

Ereigniskategorien für die Karte auswählen

Mithilfe des Filters "Ereigniskategorien" können Sie durch Auswahl der Kategorie vorgeben, welche Ereignisse auf der Karte angezeigt werden sollen.

Klicken Sie auf **Inhalt auswählen**, um das Filterformular anzuzeigen. Über das Filterformular können Sie vorgeben, welche Ereigniskategorien im Kartenportlet angezeigt werden sollen. Wenn beispielsweise eine bestimmte Ereigniskategorie für Sie von Interesse ist, die analysiert werden soll, können Sie über diesen Filter alle für Sie nicht relevanten Ereigniskategorien ausblenden. Alle Änderungen im Filterformular werden auf der Karte übernommen. Änderungen im Filterformular wirken sich auch auf die anderen Portlets in der Gruppe aus. Wird die Auswahl geändert, wird die Karte aktualisiert und es werden nur die Positionen der Ereignisse markiert, die zu den ausgewählten Kategorien gehören. Die Ereigniskategorien, die angezeigt bzw. nicht angezeigt werden sollen, werden über die Kontrollkästchen im Filterformular ausgewählt bzw. abgewählt. Um das Filterformular zu schließen, klicken Sie auf **Inhalt auswählen**. Wenn Sie die Portalseite verlassen und anschließend wieder zurückkehren, wird der Filter wieder auf die Standardauswahl zurückgesetzt, d.h., alle Kategorien sind ausgewählt.

Sie können einzelne Ereignisse hervorheben, die analysiert werden sollen, indem Sie im Portlet "Details" die entsprechenden Kontrollkästchen auswählen. Diese Ereignisse werden auf der Karte hervorgehoben.

Ressourcenfunktionen für die Karte auswählen

Bei Auswahl der Option **Ressourcen in der Nähe anzeigen** im Portlet "Details" wird der Filter "Ereigniskategorien" durch den Filter "Ressourcen" ersetzt. Über den Filter "Ressourcen" können Sie durch Auswahl nach Funktion vorgeben, welche Ressourcen auf der Karte angezeigt werden.

Klicken Sie auf **Inhalt auswählen**, um das Filterformular anzuzeigen. Über das Filterformular können Sie vorgeben, welche Ressourcenfunktionen auf der Karte und im Portlet "Details" angezeigt werden sollen. Wenn beispielsweise eine bestimmte Funktion für Sie von Interesse ist, die analysiert werden soll, können Sie über diesen Filter alle für Sie nicht relevanten Funktionen ausblenden. Alle Änderungen im Filterformular werden auf der Karte übernommen. Änderungen im Filterformular wirken sich auch auf das Portlet "Details" in derselben Gruppe aus. Wird die Auswahl geändert, wird die Karte aktualisiert und es werden nur die Positionen der Ressourcen mit den ausgewählten Funktionen auf der Karte markiert. Die Ressourcenfunktionen, die angezeigt bzw. nicht angezeigt werden sollen, werden über die Kontrollkästchen im Filterformular ausgewählt bzw. abgewählt. Um das Filterformular zu schließen, klicken Sie auf **Inhalt auswählen**. Wenn Sie die Portalseite verlassen und anschließend wieder zurückkehren, wird der Filter wieder auf die Standardauswahl zurückgesetzt, d.h., alle Funktionen sind ausgewählt. Die standardmäßig ausgewählten Funktionen hängen von der Kategorie des Ereignisses ab und davon, wie die Kategorie Funktionen zugeordnet wird.

Einstellungen der Karte zurücksetzen

Das Portlet "Karte" kann auf die für IBM Intelligent Operations Center konfigurierte Standardansicht zurückgesetzt werden.

Vorgehensweise

1. Klicken Sie im Portlet "Karte" auf **Karte zurücksetzen** oder klicken Sie auf den Pfeil in der rechten oberen Ecke.
2. Wählen Sie eine der folgenden Optionen aus:
   - **Karte zurücksetzen**, um die Karte zu vergrößern/verkleinern und gemäß der Standardeinstellung zu zentrieren.
   - **Karte und Filter zurücksetzen**, um die Karte zu vergrößern/verkleinern, gemäß der Standardeinstellung zu zentrieren und die Werte unter **Inhalt auswählen** auf die Standardwerte zurückzusetzen.

Ergebnisse

Die Karte wird entsprechend der ausgewählten Option zurückgesetzt, allerdings nur für den aktuellen Benutzer und die aktuelle Ansicht.

Ereignis hinzufügen

Sie können ein Ereignis erstellen und es gleichzeitig der Karte im Portlet "Karte" und der Liste im Portlet "Details" hinzufügen. Die Karte und die Listen ermöglichen zwei verschiedene Darstellungen desselben Inhalts.

Informationen zu diesem Vorgang

Über den Dialog **Ereignis hinzufügen** können Sie die in der folgenden Tabelle angezeigten Ereigniseigenschaften angeben:

Tabelle 92. Ereigniseigenschaften

Eigenschaft	Inhalt
Wer	
Absender	Die Quellen- oder Benutzer-ID.
Name des Ansprechpartners	Name des Ansprechpartners für weitere Informationen.
E-Mail des Ansprechpartners	E-Mail-Adresse des Ansprechpartners.
Rufnummer des Ansprechpartners	Die Telefonnummer des Ansprechpartners.
Was	
Ereignistyp*	Gibt den Ereignistyp innerhalb von *Kategorie* an.
Ereignisstatus*	Hinweise zur Behandlung von Ereignissen.
Ereignisverbreitung*	Zielgruppe, an die die Nachricht gesendet wird.
Einschränkung	Zusätzlich erforderliche Informationen, wenn "Eingeschränkt" für *Ereignisverbreitung* angegeben ist.
Kurzbeschreibung*	Eine kurze Beschreibung des Ereignisses.
Kategorie*	Allgemeine Klassifizierung von Ereignissen
Schweregrad*	Gibt den Grad der Auswirkung des Ereignisses an.
Gewissheit*	Gibt die Verlässlichkeit der Ereignisvorhersage an.
Dringlichkeit*	Zeitrahmen für die Reaktion auf das Ereignis.

Tabelle 92. Ereigniseigenschaften (Forts.)

Eigenschaft	Inhalt
Wer	
Nachrichtentyp	Gibt an, um was für eine Nachricht es sich handelt.
Beschreibung	Zusätzliche Beschreibung des Ereignisses.
Webadresse	Webadresse, unter der zusätzliche Informationen zum Ereignis zu finden sind.
Wann	
Sendedatum und -uhrzeit	Gibt an, an welchem Tag und um welche Uhrzeit die Nachricht übergeben bzw. gesendet wurde.
Wirksamkeitsdatum und -uhrzeit	Gibt an, an welchem Tag und um welche Uhrzeit die Nachricht wirksam wird.
Startdatum und - uhrzeit	Gibt an, an welchem Tag und um welche Uhrzeit das Ereignis voraussichtlich beginnt.
Ablaufdatum und -uhrzeit	Gibt an, an welchem Tag und um welche Uhrzeit das Ereignis voraussichtlich endet.
Wo	
Beschreibung des Bereichs	Beschreibung des betroffenen Bereichs.
Breitengrad und Längengrad	Koordinaten der Position des Ereignisses.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf eine Position auf der Karte und klicken Sie auf **Ereignis hinzufügen**, um den Dialog **Ereignis hinzufügen** zu öffnen. Einige Ereigniseigenschaften werden automatisch angegeben.
2. Geben Sie alle anderen Ereigniseigenschaften über die im Dialog enthaltenen Felder an. Die mit einem Stern (*) markierten Eigenschaften müssen angegeben werden, damit ein neues Ereignis erstellt werden kann. Die Angabe der nicht markierten Eigenschaften ist optional.
3. Klicken Sie auf **OK**, um das Ereignis zu speichern, oder klicken Sie auf **Abbrechen**, wenn das Ereignis nicht hinzugefügt werden soll.

Ergebnisse

An der vorgegebenen Position auf der Karte wird ein Symbol für die Kategorie des neuen Ereignisses angezeigt. Die Details zu dem neuen Ereignis finden Sie in der Liste des verknüpften Portlets "Details".

Portlet "Karte" anpassen

Administrator

Wenn Sie Administratorzugriff besitzen, können Sie dieses Portlet anpassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Die Portlets "Karte" und "Positionskarte" können ebenfalls über Änderungen an globalen Einstellungen angepasst werden. Über globale Einstellungen wird der Inhalt des Portlets für alle Benutzer und alle Portletinstanzen vorgegeben. Globale Einstellungen werden durch gemeinsam genutzte Einstellungen außer Kraft gesetzt.

Die folgenden Einstellungen für das Portlet "Karte" können geändert werden:

- Sie können den Standardmittelpunkt und die Standardzoomstufe für die Karte zurücksetzen.
- Sie könne eine neue Basiskarte auswählen; standardmäßig wird eine ArcGIS-Karte von Esri verwendet.

- Sie können der Karte geografische Beschriftungen und Visualisierungsebenen in KML (Keyhole Markup Language) zur Darstellung zusätzlicher Daten hinzufügen.
- Sie können einen Schwellenwert für die Anzahl der Markierungen definieren, die ohne einen Warnhinweis angezeigt werden können.
- Sie können in den Kartenfiltern die Standardauswahl definieren, die bei Klicken auf **Inhalt auswählen** angezeigt werden soll.
- Sie können den Namen der Gruppe angeben, der eine Kommunikation mit anderen Kartenportlets und Details-Portlets ermöglicht.

Sie können generische Portletparameter setzen, die für alle Portlets gelten (den Verzeichnispfad der Hilfedatei, die Höhe des Portlets, den Portlet-Titel und das Ressourcenpaket).

Zugehörige Verweise:

„Einstellungen des Karte-Portlets" auf Seite 166
Anpassen des Karte-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Meine Aktivitäten

Im Portlet "Meine Aktivitäten" wird eine dynamische Liste mit Aktivitäten angezeigt, deren Eigner die Gruppe ist, zu der der an der Schnittstelle angemeldete Benutzer gehört.

Jedes Mal, wenn ein Ereignis aufgrund eines in der Auswahlmatrix für Standard Operating Procedure definierten Auswahlkriteriums eine SOP (Standard Operating Procedure) auslöst, werden die zugehörigen Aktivitäten Eignern zugeordnet. Weitere Informationen zu Standard Operating Procedures erhalten Sie über den Link am Ende des Themas.

Angemeldete Benutzer können die ihnen zugeordneten Aktivitäten im Portlet "Meine Aktivitäten" anzeigen. Im Portlet "Meine Aktivitäten" sind die Aktivitäten nach übergeordneten SOPs (Standard Operating Procedures) angeordnet. Jede Standard Operating Procedure entspricht einem Ereignis.

Im Portlet "Meine Aktivitäten" werden nur die offenen Aktivitäten für die einzelnen Standard Operating Procedures angezeigt, nicht die geschlossenen oder abgeschlossenen Aktivitäten. Zu offenen Aktivitäten gehören Aktivitäten, die bereits gestartet wurden, sowie Aktivitäten, die gestartet werden können. Sind beispielsweise in einer Standard Operating Procedure eine oder auch mehrere Aktivitäten nacheinander angeordnet, wird nur jeweils die aktuelle Aktivität angezeigt. Kann eine Aktivität erst nach Abschluss einer vor ihr anstehenden Aktivität ausgeführt werden, wird sie erst ausgeführt, wenn die Vorgängeraktivität abgeschlossen ist oder übersprungen wurde.

Oben im Portlet "Meine Aktivitäten" werden folgende Symbole zum Status von Aktivitäten angezeigt:

Verstrichen
: Aktivitäten, deren Ausführung überfällig ist.

Heute Aktivitäten, die heute noch ausgeführt werden müssen.

In der Zukunft
: Aktivitäten, die zu einem späteren Zeitpunkt ausgeführt werden müssen.

Nach dem Start einer Aktivität wird ihr Fälligkeitsdatum berechnet, indem Startzeit und Ausführungsdauer addiert werden. Anhand des Fälligkeitsdatums von Aktivitäten wird die Zahl errechnet, die dann in den einzelnen Fälligkeitssymbolen angezeigt wird.

Im Portlet "Meine Aktivitäten" werden zuerst Standard Operating Procedures mit überfälligen Aktivitäten angezeigt. Die verbleibenden Standard Operating Procedures werden danach in alphabetischer Reihenfolge angezeigt.

In der Liste mit überfälligen Aktivitäten wird neben jeder Standard Operating Procedure ein rotes Symbol mit einer Zahl angezeigt, die die Anzahl der überfälligen Aktivitäten angibt. Die Reihenfolge der Standard Operating Procedures mit überfälligen Aktivitäten richtet sich nach der Anzahl der jeweils darin enthaltenen überfälligen Aktivitäten. Die Standard Operating Procedure mit den meisten überfälligen Aktivitäten steht in der Liste ganz oben.

Aktivitäten im Portlet "Meine Aktivitäten" verwalten

Im Portlet "Meine Aktivitäten" sind folgende Schritte für Ihre Aktivitäten möglich:

- Sie können Details zu einer Standard Operating Procedure anzeigen, indem Sie den Namen der betreffenden Standard Operating Procedure erweitern.
  - Der Name des Ereignisses, von dem die Standard Operating Procedure ausgelöst wurde, wird angezeigt. Wenn Sie den Cursor über den Namen des Ereignisses bewegen, wird eine Kurzinfo mit Startdatum und -zeit sowie Kategorie, Schweregrad, Gewissheit (Eintrittswahrscheinlichkeit) und Dringlichkeit angezeigt.
  - Wird das Portlet "Details" auf der Seite angezeigt, klicken Sie auf den Namen des Ereignisses, um die Ereigniseigenschaften anzuzeigen. Das Ereignisfenster **Eigenschaften** wird geöffnet.
  - Es werden die Schritte angezeigt, die gerade ausgeführt werden bzw. die gestartet werden können. Darüber hinaus werden Status und Fälligkeitsdatum der einzelnen Schritte angezeigt.
- Sie können weitere Details zu einem Schritt anzeigen (einschließlich der Kommentare und Verweise, die dem Schritt von den Benutzern hinzugefügt wurden), indem Sie den Namen des betreffenden Schritts erweitern.
- Sie können einen Schritt starten, beenden oder überspringen, indem Sie den Namen des betreffenden Schritts erweitern und anschließend eine der folgenden Optionen auswählen:
  - Um einen Schritt zu starten, wählen Sie in der Liste **Start** (Starten) aus. Ist der Schritt in der Standard Operating Procedure als automatische Task definiert, wird der dieser Task zugeordnete Workflow automatisch gestartet. Der Schritt selbst wird automatisch beendet. Der Benutzer, der einen Schritt startet, wird automatisch Eigner dieses Schritts und der Name dieses Benutzers wird im Feld **Eigner** angezeigt.
  - Um einen Schritt zu überspringen, wählen Sie in der Liste **Skip** (Überspringen) aus.
  - Um einen Schritt zu beenden, wählen Sie in der Liste **Finish** (Fertigstellen) aus.
- Um einen Schritt mit einem Kommentar zu versehen, führen Sie die folgenden Unterschritte aus:
  1. Erweitern Sie den Namen des Schritts.
  2. Wählen Sie in der Liste **Add Comment** (Kommentar hinzufügen) aus.
  3. Geben Sie im Feld **Comment** (Kommentar) des Fensters **Add Comment** (Kommentar hinzufügen) einen Kommentar ein. Die Felder **Commentator name** (Name des Kommentators) und **Activity name** (Name der Aktivität) sind schreibgeschützt und enthalten automatisch eingetragene Werte.
  4. Klicken Sie auf **OK**.
  5. Erweitern Sie erneut den Namen des Schritts. Der neue Kommentar wird ganz unten in der Liste der bereits vorhandenen Kommentare und Verweise für den Schritt angezeigt.
- Um einen Schritt mit einem Verweis zu versehen, führen Sie die folgenden Unterschritte aus:
  1. Erweitern Sie den Namen des Schritts.
  2. Wählen Sie in der Liste **Add Reference** (Verweis hinzufügen) aus.
  3. Geben Sie im Fenster **Add Reference** (Verweis hinzufügen) Werte für **Reference name** (Name des Verweises) und **Reference URI** (Verweis-URI) ein. Das Feld **Activity name** (Name der Aktivität) ist schreibgeschützt und enthält einen automatisch eingetragenen Wert.
  4. Klicken Sie auf **OK**.
  5. Erweitern Sie erneut den Namen des Schritts. Der neue Verweis wird als Link ganz unten in der Liste der bereits vorhandenen Kommentare und Verweise für den Schritt angezeigt.

- Sie können Details zu der Standard Operating Procedure anzeigen, indem Sie auf das Symbol **i** neben der Standard Operating Procedure klicken. Im Fenster **Standard Operating Procedure Details** (SOP-Details) werden alle in der Standard Operating Procedure enthaltenen Aktivitätsschritte angezeigt; dazu gehören alle Schritte, die gerade ausgeführt werden oder gestartet werden können, sowie die abgeschlossenen Schritte und die Schritte, die geschlossen wurden. Darüber hinaus werden Status und Fälligkeitsdatum der einzelnen Schritte angezeigt. Sie können weitere Details zu einem Schritt anzeigen, indem Sie den Namen des betreffenden Schritts erweitern.

Administrator

Portlet "Meine Aktivitäten" anpassen

Wenn Sie Administratorzugriff besitzen, können Sie dieses Portlet anpassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Für das Portlet "Meine Aktivitäten" können Sie einen Gruppennamen angeben, um die Kommunikation mit anderen Portlets zu ermöglichen, beispielsweise mit Portlets des Typs "Details".

Sie können generische Portletparameter setzen, die für alle Portlets gelten (den Verzeichnispfad der Hilfedatei, die Höhe des Portlets, den Portlet-Titel und das Ressourcenpaket).

Zugehörige Konzepte:

„Standard Operating Procedures” auf Seite 135
Für die Verwaltung von Ereignissen, die im IBM Intelligent Operations Center auftreten, können Sie Standard Operating Procedures und Aktivitäten definieren. Verwenden Sie das Portlet "Standard Operating Procedures", um auf Standard Operating Procedure, Auswahlmatrix für Standard Operating Procedure und Workflow-Designer-Anwendungen in Tivoli Service Request Manager zuzugreifen.

Zugehörige Verweise:

„Einstellungen des Meine Aktivitäten-Portlets” auf Seite 169
Anpassen des Meine Aktivitäten-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Benachrichtigungen

Mit dem Portlet "Benachrichtigungen" können Sie Alertnachrichten sowie Details zu diesen Nachrichten anzeigen.

Bei dem Portlet "Benachrichtigungen" handelt es sich um ein interaktives Fenster, das eine Liste aller für Sie relevanten aktuellen Alerts enthält. Sie können nur die Alerts sehen, die an Benutzergruppen gesendet wurden, in denen Sie Mitglied sind. Alerts sind Benachrichtigungen, die in den folgenden Fällen empfangen werden:

- Innerhalb eines Bereichs treten ungefähr zeitgleich mehrere Ereignisse auf, die unter Umständen in Konflikt miteinander stehen oder eine Koordination erforderlich machen.
- Ein KPI (Key Performance Indicator) hat einen vom Administrator als Auslöser für einen Alarm vordefinierten Wert angenommen.

Darüber hinaus können Sie mit diesem Portlet weitere Informationen zu einem Alert anzeigen.

Benachrichtigungen - Liste

Das Portlet "Benachrichtigungen" stellt eine dynamische, interaktive Liste der Alerts bereit, die aufgrund geänderter KPI-Werte und damit in Zusammenhang stehender Ereignisse ausgegeben werden. Dieses Portlet hat die Aufgabe, auf Änderungen von KPI-Werten oder des Ereignisstatus hinzuweisen. Die Liste enthält wichtige Angaben zu jedem Alert.

Wenn Sie den Cursor über eine Zeile bewegen, wird eine ausführlichere Beschreibung dieses Alerts angezeigt. Sollen alle Informationen in Zusammenhang mit einem Alert in einem Fenster angezeigt werden, klicken Sie mit der rechten Maustaste auf die betreffende Zeile und wählen Sie **Eigenschaften** aus.

Wenn Sie die Portalseite öffnen, werden im Portlet zunächst alle Ihre aktuellen Alerts angezeigt. Sie können Alerts aus dem Portlet entfernen, indem Sie mit der rechten Maustaste auf die betreffende Zeile klicken und **Alert schließen** auswählen. Sie können mehrere Alerts gleichzeitig schließen, indem Sie mehrere Zeilen auswählen. Schließen Sie ein Alert erst, nachdem es entsprechend behandelt wurde, da es beim Schließen für alle Empfänger entfernt wird.

Klicken Sie auf die Schaltfläche in der rechten oberen Ecke des Fensters, um es zu schließen und zur Liste zurückzukehren.

Ein Zähler in der linken Ecke der Aktionsleiste am Ende der Liste gibt die Anzahl der Elemente, die angezeigt werden, sowie die Anzahl der Elemente insgesamt an. In der Mitte der Aktionsleiste können Sie die Anzahl der Elemente auswählen, die gleichzeitig angezeigt werden sollen. Sind mehr Zeilen vorhanden, als gleichzeitig angezeigt werden können, können Sie die Seite über die Schaltflächen in der rechten Ecke der Aktionsleiste nach oben bzw. nach unten verschieben.

Alerteigenschaften

Im Fenster mit den Alertdetails werden die folgenden Eigenschaften angezeigt:

Tabelle 93. Alerteigenschaften

Eigenschaft	Inhalt
Überschrift	Kurze Beschreibung des Alerts
Kategorie	Allgemeine Klassifizierung eines Ereignisses oder KPI
Absender	Quelle des Alerts
Gesendet an Gruppen	Die Gruppen, an die der Alert gesendet wurde
Gesendet	Datum und Uhrzeit, zu der der Alert gesendet wurde
Beschreibung	Zusätzliche Angaben zum Alert
Bezieht sich auf Alerts	Ereignis-ID, wenn der Alert durch zugehörige Ereignisse ausgelöst wird
Bezieht sich auf KPIs	Name des KPI, wenn der Alert durch die Änderung eines KPI-Werts ausgelöst wird

Administrator

Portlet "Benachrichtigungen" anpassen

Wenn Sie Administratorzugriff besitzen, können Sie dieses Portlet anpassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Über die Parameter für das Portlet "Benachrichtigungen" können Sie folgende Einstellungen vornehmen:

- Geben Sie Spaltenanordnung, Überschriften, Sortierreihenfolge und Priorität an.
- Blenden Sie die Symbolleiste oben in der Liste ein bzw. blenden Sie sie aus.

Sie können generische Portletparameter setzen, die für alle Portlets gelten (den Verzeichnispfad der Hilfedatei, die Höhe des Portlets, den Portlet-Titel und das Ressourcenpaket).

Zugehörige Verweise:

„Einstellungen des Benachrichtigungen-Portlets" auf Seite 169
Anpassen des Benachrichtigungen-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Berichte

Mit dem Portlet "Berichte" können Berichte von Ereignissen in Form von Diagrammen angezeigt werden. In diesem Portlet gibt es mehrere Möglichkeiten für die Anordnung von Ereignissen; darüber hinaus können Ereignisse nach einem bestimmten Datum oder Zeitraum ausgewählt werden. Mithilfe dieser Berichte können Sie Maßnahmen für aktuelle und künftige Ereignisse planen.

Berichte erstellen

Mithilfe des Berichtsportlets können Sie für Ereignisse einen benutzerdefinierten Bericht erstellen. Wählen Sie dazu zunächst aus, wie die Ereignisse gruppiert werden sollen. Sollen beispielsweise alle Ereignisse angezeigt werden, die zu einer bestimmten Kategorie gehören, wählen Sie in dem Feld, in dem die Anordnung der Ereignisse angegeben werden kann, die Option **Kategorie** aus. Dann können Sie in den Feldern für die Auswahl der Daten die Daten in Zusammenhang mit den Informationen eingeben, die angezeigt werden sollen. Darüber hinaus können Sie für die Ereignisse im Bericht ein bestimmtes Datum oder einen bestimmten Zeitraum angeben. Wenn Sie anschließend auf **Aktualisieren** klicken, werden im Diagramm die gewünschten Informationen angezeigt.

Um die URL für den neuen Bericht abzurufen, klicken Sie auf die Option zum Abruf der Berichts-URL.

In Tabelle 1 sind die Kriterien aufgeführt, nach denen Ereignisse angeordnet werden können.

Tabelle 94. Benutzerdefinierter Bericht

Anordnen nach	Beschreibung
Ereignistyp	Zeigt die Ereignisse nach Typ an. So kann es sich bei einem Ereignis beispielsweise um einen heraufziehenden Wirbelsturm oder einen Verkehrsunfall handeln.
Schweregrad	Zeigt Ereignisse nach Schweregrad an. Ereignisse können beispielsweise als "Extrem" oder "Schwerwiegend" eingestuft werden.
Gewissheit	Zeigt Ereignisse nach der Wahrscheinlichkeit an, mit der sie auftreten werden. Ist es beispielsweise zu einem Verkehrsunfall gekommen, ist die Gewissheit "Beobachtet".
Dringlichkeit	Zeigt Ereignisse nach ihrer Dringlichkeit an. So kann das Ereignis beispielsweise auftreten und mit dem Begriff "sofort" beschrieben werden.
Ereigniskategorie	Zeigt Ereignisse nach Ereigniskategorie an. So können Sie beispielsweise alle Ereignisse in Zusammenhang mit Umwelt, Feuer oder Transport anzeigen.
Nachrichtentyp	Zeigt Ereignisse nach Nachrichtentyp (z. B. Aktualisierungen oder Alerts) an.
Status	Zeigt Ereignisse nach Status an. Für den Status kann Folgendes angegeben werden: • Akzeptabel • Vorsicht • Take action (Maßnahme ergreifen)

Tabelle 94. Benutzerdefinierter Bericht (Forts.)

Anordnen nach	**Beschreibung**
Absender	Zeigt Ereignisse nach einem bestimmten Sender an. So kann es sich bei dem Ereignis beispielsweise um ein Sicherheitsproblem oder um ein Problem handeln, das IBM Intelligent Operations for Water betrifft.
Vorfall	Zeigt Ereignisse nach Vorfallstyp an. So können beispielsweise alle Verkehrsunfälle oder Straßenbauarbeiten angezeigt werden.
Bearbeitungscode	Zeigt Ereignisse nach Bearbeitungscode an. Beispiel für einen Bearbeitungscode ist "Ereignis".
Sender Name (Sendername)	Zeigt Ereignisse nach dem Namen des Senders an.

In Tabelle 2 sind die Daten aufgeführt, die für den Bericht ausgewählt werden können.

Tabelle 95. Daten auswählen

Daten auswählen	**Beschreibung**
Schweregrad	Zeigt Ereignisse nach Schweregrad an. Ereignisse können beispielsweise als "Extrem" oder "Schwerwiegend" eingestuft werden.
Gewissheit	Zeigt Ereignisse nach der Wahrscheinlichkeit an, mit der sie auftreten werden. Ist es beispielsweise zu einem Verkehrsunfall gekommen, ist die Gewissheit "Beobachtet".
Dringlichkeit	Zeigt Ereignisse nach ihrer Dringlichkeit an. So kann das Ereignis beispielsweise auftreten und mit dem Begriff "sofort" beschrieben werden.
Ereigniskategorie	Zeigt Ereignisse nach Ereigniskategorie an. So können Sie beispielsweise alle Ereignisse in Zusammenhang mit Umwelt, Feuer oder Transport anzeigen.
Ereignistyp	Zeigt die Ereignisse nach Typ an. So kann es sich bei einem Ereignis beispielsweise um einen heraufziehenden Wirbelsturm oder einen Verkehrsunfall handeln.
Anfangsdatum	Geben Sie das Datum an, für das Ereignisse angezeigt werden sollen. Bei Angabe eines Zeitraums wird hier das Anfangsdatum eingegeben.
Enddatum	Geben Sie hier das Datum ein, bis zu dem Ereignisse angezeigt werden sollen.

Anmerkung: Damit dieses Portlet wie erwartet funktioniert, müssen Sie sich am Lösungsportal mit dem vollständig qualifizierten Domänennamen des IBM Intelligent Operations Center-Anwendungsservers anmelden. Wenn Sie sich mit einer IP-Adresse oder einem Hostnamenalias anstatt mit dem registrierten, vollständig qualifizierten Domänennamen am Portal anmelden, wird dieses Portlet nicht ordnungsgemäß angezeigt.

Berichts-URL kopieren

Soll eine Berichts-URL kopiert und der Bericht rechts im Portlet in einem Rahmen angezeigt werden, klicken Sie mit der rechten Maustaste auf die URL und wählen Sie die Option zum Kopieren der Linkadresse aus. Die genaue Bezeichnung dieser Option hängt von dem von Ihnen verwendeten Browser ab.

Wichtig:
Um einen benutzerdefinierten Bericht zu speichern und den hier kopierten Link zu verwenden, geben Sie

im Feld **Anfangsdatum** das gestrige Datum und im Feld **Enddatum** das morgige Datum ein. Mit diesen Datumsangaben wird sichergestellt, dass Sie alle Daten abrufen, die Sie in den benutzerdefinierten Bericht einschließen möchten. Wenn Sie beispielsweise den Datumsbereich 10.08.2012 bis 18.08.2012 verwenden möchten, geben Sie für die Filterkriterien folgende Datumsangaben ein:

- Anfangsdatum - 09.08.2012
- Enddatum - 19.08.2012

Berichtsbeispiele

In IBM Intelligent Operations Center ist das Portlet "Berichte" bereitgestellt, das Berichte enthält, die anhand der im Portlet "Ereignisse" enthaltenen Daten grafisch aufbereitet sind.

Im großen Berichtsfenster werden die Parameter für die Informationen ausgewählt, die im Berichtsdiagramm angezeigt werden sollen.

In die beiden Fenster rechts im Portlet werden benutzerdefinierte Berichte kopiert.

Bei den Berichten unten auf der Seite handelt es sich um vordefinierte Diagramme. Sollen Ereignisse in diesen Berichten nach Datum oder Zeitraum angezeigt werden, klicken Sie auf **Bericht konfigurieren**. Geben Sie das gewünschte Datum bzw. den Zeitraum ein und klicken Sie auf die Option zum Anzeigen des Berichts

Berichtsintegration

Im Portlet "Berichte" wird ein I-Frame bereitgestellt, mit dem IBM Cognos Business Intelligence-Berichte oder -Seiten eingebettet werden können. Geben Sie die URL des Berichts oder der Seite an, der bzw. die in das Portlet integriert werden soll.

Administrator

Portlet "Berichte" anpassen

Wenn Sie Administratorzugriff besitzen, können Sie dieses Portlet anpassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Sie können generische Portletparameter setzen, die für alle Portlets gelten (den Verzeichnispfad der Hilfedatei, die Höhe des Portlets, die Breite des Portlets und den Portlet-Titel). Darüber hinaus können Sie die URL des angezeigten Berichts angeben.

Zugehörige Verweise:

„Einstellungen des Berichte-Portlets” auf Seite 172
Anpassen des Berichte-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Status

Mit dem Portlet "Status" können Sie den Status von KPIs einer einzelnen Einrichtung oder mehrerer Einrichtungen anzeigen.

Das Portlet "Status" stellt eine für Entscheidungsträger hilfreiche Statusübersicht der KPIs aller Einrichtungen bereit, für die eine Anzeigeberechtigung erteilt wurde. In diesem Portlet können Sie aktuelle Änderungen am KPI-Status anzeigen und damit planen und bei Bedarf entsprechende Maßnahmen vornehmen.

KPI-Farbcode

Jede Spalte enthält KPI-Informationen zu einer Einrichtung, deren Name oben in der Spalte steht. Die den einzelnen Einrichtungen zugeordneten KPI-Kategorien werden anhand farbiger Zellen dargestellt. Die Hintergrundfarbe einer KPI-Kategorie zeigt deren Status an. Sollen in einer Spalte mehr als sechs KPIs angezeigt werden, wird die Größe der einzelnen Zellen entsprechend angepasst, um Raum für die zusätzlichen KPIs zu schaffen.

Die Codes für die Hintergrundfarben der Beispiel-KPIs in der Lösung haben folgende Bedeutung:

- Grün: Gibt an, dass der Status auf Basis der Parameter für den betreffenden KPI zulässig ist.
- Gelb: Gibt an, dass Vorsicht geboten und eine Überwachung erforderlich ist.
- Rot: Gibt an, dass entsprechende Maßnahmen empfohlen werden.
- Grau: Gibt an, dass die vorliegenden Daten nicht ausreichen, um den KPI-Status zu ermitteln.

Der Farbcode ist in der Legende oben im Portlet definiert.

Ein nicht bestimmbarer Status deutet darauf hin, dass für den Zeitraum, der für den betreffenden KPI definiert ist, kein KPI-Wert verfügbar ist. Dies ist der Fall, wenn die Lösung innerhalb des angegebenen Zeitraums keine Nachrichten für den KPI empfängt. So wird beispielsweise der Wasserstand für eine Wasserquelle täglich berechnet. Wird an einem Tag keine Nachricht zum Wasserstand dieser Wasserquelle empfangen, sind keine Daten vorhanden, mit deren Hilfe der KPI-Wert ermittelt werden kann.

Um den KPI-Namen und eine Definition des durch die Farbe des KPI angegebenen Status anzuzeigen, bewegen Sie den Cursor über die Zelle.

KPI-Aktualisierungen

Wenn sich Änderungen an einem KPI ergeben, wird dies im Portlet "Status" angezeigt. Angenommen, der Status einer der Beispiel-KPIs, die den Status des KPI für die Wasserqualität festlegen, wechselt von "Akzeptabel" zu "Vorsicht". Diese Änderung wird im Portlet wiedergegeben, indem die Hintergrundfarbe der Zelle mit der Wasserqualität von grün zu gelb wechselt. Darüber hinaus wird auch im Portlet "Benachrichtigungen" angezeigt, dass sich an einem KPI eine Änderung ergeben hat.

Erhält die Lösung eine Nachricht zur Berechnung eines KPI, erfolgt umgehend eine Farbänderung. Diese Funktion ist von Vorteil, wenn für die KPI-Kategorie häufig Änderungen in Echtzeit eingehen (beispielsweise bei Verspätungen im Flugverkehr). Dagegen ist diese Funktion unerheblich für Kategorien mit archivierten (historischen) KPIs wie beispielsweise beim Hochwasserschutz. Bei diesen KPI-Kategorien werden tägliche Messungen vorgenommen und es sind keine plötzlichen Änderungen zu erwarten, die sich sich nachhaltig auf den Status auswirken.

Für jeden KPI werden im Portlet "Key Performance Indicator - Drilldown" (das mit dem Portlet "Status" verknüpft ist) alle zugrunde liegenden KPIs und deren Details angezeigt.

Soll im Portlet "Key Performance Indicator - Drilldown" nur ein bestimmter KPI angezeigt werden, klicken Sie in der Tabelle im Portlet "Status" auf die Zeile des KPI. Wenn Sie auf den Titel der Eignereinrichtung (beispielsweise "Wasser") klicken, werden alle relevanten KPIs angezeigt.

Administrator

Portlet "Status" anpassen

Wenn Sie Administratorzugriff besitzen, können Sie dieses Portlet anpassen. Klicken Sie dazu in die rechte obere Ecke des Portlets, um das Portletmenü mit den Anpassungsoptionen anzuzeigen. Gemeinsam genutzte Einstellungen wirken sich für alle Benutzer auf den Portletinhalt aus, jedoch nur für diese Portletinstanz.

Über die Parameter für das Portlet "Status" können Sie folgende Einstellungen vornehmen:

- Die Farben für die KPIs anpassen.
- Weitere KPI-Filter aktivieren.
- Die KPI-Legende ein- bzw. ausblenden.
- Die Sortierreihenfolge der KPIs definieren.
- Einen Gruppennamen angeben, um die Kommunikation mit dem Portlet "Key Performance Indicator - Drilldown" zu ermöglichen.

Sie können generische Portletparameter setzen, die für alle Portlets gelten (den Verzeichnispfad der Hilfedatei, die Höhe des Portlets, den Portlet-Titel und das Ressourcenpaket).

KPIs anpassen

In der Lösung stehen mehrere Beispiel-KPIs bereit. Diese KPIs sollen bei der Planung und Implementierung verschiedener, für Ihre Einrichtung relevanter KPIs helfen. Es werden Beispiele aus dem Bereich Wasser, Transport und öffentliche Sicherheit bereitgestellt.

Zugehörige Konzepte:

„Key Performance Indicators (KPIs)” auf Seite 178
Mit dem Portlet "Key Performance Indicators (KPIs)" können Sie KPIs (Key Performance Indicator) und ihre hierarchische Anzeige in IBM Intelligent Operations Center anpassen.

Zugehörige Verweise:

„Einstellungen des Status-Portlets” auf Seite 174
Anpassen des Status-Portlets durch Änderung der Einstellungen in den Feldern des Fensters **Gemeinsam genutzte Einstellungen**.

Kapitel 9. Fehlersuche und Unterstützung

Zur Eingrenzung und Lösung von Problemen in Verbindung mit Ihrer IBM Software können Sie die Informationen zur Fehlersuche und zur Unterstützung verwenden. Dort finden Sie Anweisungen zur Verwendung der Fehlerbestimmungsressourcen, die gemeinsam mit Ihren IBM Produkten bereitgestellt werden.

Verfahren für die Fehlersuche bei Problemen

Die Fehlersuche ist ein systematischer Ansatz zur Lösung eines Problems. Mit der Fehlersuche soll festgestellt werden, weshalb etwas nicht wie erwartet funktioniert und wie das Problem gelöst werden kann.

Der erste Schritt des Fehlersuchprozesses besteht in der vollständigen Beschreibung des Problems. Eine gute Problembeschreibung ist wichtig, damit Sie und der zuständige IBM Technical Support-Mitarbeiter wissen, wo die Ursache des Problems zu suchen ist. Unter anderem müssen Sie sich in diesem Schritt einige Grundsatzfragen stellen:

- Wie lauten die Symptome des Problems?
- Wo tritt das Problem auf?
- Wann tritt das Problem auf?
- Unter welchen Bedingungen tritt das Problem auf?
- Kann das Problem erneut generiert werden?

Normalerweise liefern die Antworten auf diese Fragen bereits eine gute Beschreibung des Problems, was dann wiederum eine Problemlösung ermöglichen kann.

Wie lauten die Symptome des Problems?

Bei der Beschreibung eines Problems stellt sich zunächst die offensichtliche Frage „Worin liegt das Problem?" Diese Frage erscheint möglicherweise etwas zu allgemein, allerdings können Sie diese Frage in einige präzisere Einzelfragen unterteilen, die möglicherweise eine genauere Vorstellung des Problems liefern. Im Folgenden werden beispielhaft einige dieser Fragen genannt:

- Von wem oder was wurde das Problem gemeldet?
- Wie lauten die Fehlercodes und Nachrichten?
- Wie schlägt das System fehl? Handelt es sich beispielsweise um eine Endlosschleife, eine Blockierung, einen Absturz, eine Leistungsbeeinträchtigung oder um ein falsches Ergebnis?

Wo tritt das Problem auf?

Die Ermittlung der Fehlerquelle ist nicht immer einfach, ist jedoch einer der wichtigsten Schritte beim Lösen eines Problems. Zwischen der Meldung und den fehlschlagenden Komponenten können viele Technologieebenen liegen. Bei der Untersuchung von Problemen müssen neben vielen weiteren Faktoren beispielsweise Netzwerke, Datenträger und Treiber überprüft werden.

Mithilfe der folgenden Fragen können Sie sich darauf konzentrieren, wo das Problem auftritt und so die Problemebene eingrenzen:

- Tritt das Problem nur bei einer bestimmten Plattform oder einem bestimmten Betriebssystem auf, oder wurde es auf mehreren Plattformen oder Betriebssystemen festgestellt?
- Werden die derzeitige Umgebung und Konfiguration unterstützt?

Das Problem muss nicht notwendigerweise in der Ebene seine Ursache haben, die das Problem meldet. Damit Sie bestimmen können, wo das Problem seinen Ursprung hat, müssen Sie die Umgebung kennen, in der es auftritt. Nehmen Sie sich die Zeit, die Problemumgebung ausführlich zu beschreiben, einschließlich des Betriebssystems und der Version, der gesamten entsprechenden Software mit allen Versionen und der Hardwaredaten. Vergewissern Sie sich, dass Sie das Produkt in einer Umgebung mit einer unterstützten Konfiguration ausführen; häufig sind Probleme auf nicht kompatible Softwareversionen zurückzuführen, die nicht gemeinsam ausgeführt werden können oder deren gemeinsame Ausführung nicht umfassend getestet wurde.

Wann tritt das Problem auf?

Arbeiten Sie einen detaillierten Zeitplan der Ereignisse aus, die zu einem Fehler führen - dies gilt insbesondere in Fällen, die nur einmalig auftraten. Am einfachsten arbeiten Sie sich hierfür Schritt für Schritt zurück: Beginnen Sie bei dem Zeitpunkt, zu dem der Fehler gemeldet wurde (so genau wie möglich, unter Umständen sogar bis auf die letzte Millisekunde), und arbeiten Sie sich dann zurück durch die verfügbaren Protokolle und Informationen. Für gewöhnlich müssen Sie nur bis zum ersten fehlerverdächtigen Ereignis zurückspringen, das Sie in einem Diagnoseprotokoll finden.

Beantworten Sie folgende Fragen, um einen ausführlichen Zeitplan der Ereignisse auszuarbeiten:

- Tritt das Problem nur zu einer bestimmten Tages- oder Nachtzeit auf?
- Wie häufig tritt das Problem auf?
- Welche Ereignisfolge findet bis zu dem Zeitpunkt statt, zu dem das Problem gemeldet wurde?
- Tritt das Problem nach einer Umgebungsänderung auf, beispielsweise wenn Software oder Hardware aufgerüstet oder installiert wurde?

Die Beantwortung derartiger Fragen ermöglicht einen Referenzrahmen, innerhalb dessen das Problem untersucht werden kann.

Unter welchen Bedingungen tritt das Problem auf?

Für die Fehlersuche ist es wichtig, zu wissen, welche Systeme und Anwendungen ausgeführt wurden, als das Problem auftrat. Diese Fragen zu Ihrer Umgebung können bei der Bestimmung der Fehlerursache hilfreich sein:

- Tritt das Problem immer auf, wenn dieselbe Task ausgeführt wird?
- Muss eine bestimmte Ereignisfolge ablaufen, damit das Problem auftritt?
- Schlagen zur selben Zeit auch andere Anwendungen fehl?

Durch die Beantwortung dieser Art von Fragen kann die Umgebung, in der das Problem auftritt, verdeutlicht werden, und eventuelle Abhängigkeiten lassen sich möglicherweise erkennen. Denken Sie daran, dass Probleme, die ungefähr zum selben Zeitpunkt auftraten, nicht unbedingt miteinander in Zusammenhang stehen müssen.

Kann das Problem erneut generiert werden?

Für die Fehlersuche ist ein erneut generierbares Problem ideal. Für gewöhnlich stehen für erneut generierbare Probleme mehr Tools oder Prozeduren für die Untersuchung zur Verfügung. Folglich sind erneut generierbare Probleme häufig einfacher zu testen und zu lösen. Erneut generierbare Probleme können jedoch auch von Nachteil sein: Wenn das Problem einen entscheidenden Einfluss auf die Geschäftsabläufe hat, sollte es nicht erneut auftreten. Falls möglich, generieren Sie das Problem erneut in einer Test- oder Entwicklungsumgebung, die für gewöhnlich mehr Flexibilität und Kontrolle während der Untersuchung bietet.

- Kann das Problem auf einem Testsystem erneut generiert werden?
- Tritt dieselbe Art von Problem bei mehreren Benutzern bzw. Anwendungen auf?

- Kann das Problem durch die Ausführung eines einzelnen Befehls oder einer Befehlsgruppe oder durch die Ausführung einer bestimmten Anwendung erneut generiert werden?

Referenzinformationen

„Wissensdatenbanken durchsuchen" auf Seite 341
Durch eine Suche in den Wissensdatenbanken von IBM lassen sich häufig Probleme lösen. Mithilfe verfügbarer Ressourcen, Unterstützungstools und Suchmethoden können Sie Ihre Ergebnisse optimieren.

Tracing aktivieren und Protokolldateien anzeigen

Zur Fehlerbehebung bei Problemen im IBM Intelligent Operations Center müssen Sie möglicherweise Protokolldateien in mehreren Systemen analysieren. In den folgenden Themen erfahren Sie, wie Sie auf die Protokolldateien zugreifen können.

Um die Traces zu starten und die Protokolle anzuzeigen, geben Sie die Befehle zur Laufzeit als Rootbenutzer ein.

Zugehörige Konzepte:

„Komponenten überprüfen" auf Seite 220
Mit dem Systemprüfungstool wird überprüft, ob auf die Komponenten in IBM Intelligent Operations Center zugegriffen werden kann und ob sie betriebsbereit sind.

„IBM Support Assistant Lite installieren und verwenden" auf Seite 320
Das Tool IBM Support Assistant Lite (ISA Lite) sammelt gängige Diagnosedaten, die bei der Analyse allgemeiner Probleme hilfreich sind.

Zugehörige Tasks:

„MustGather-Tool bei der Installation ausführen" auf Seite 316
Es werden Protokolldateien erstellt, während IBM Intelligent Operations Center installiert wird. Es ist ein Tool verfügbar, das diese Protokolldateien zur Analyse zusammenstellt.

Protokolldateien des Anwendungsservers

Mit den folgenden Prozeduren können Sie für einige der Systeme auf dem Anwendungsserver das Tracing aktivieren und Protokolle anzeigen.

Anhand der folgenden Prozeduren wird beschrieben, wie Sie für die folgenden Systeme das Tracing aktivieren und Protokolle anzeigen können:

- WebSphere Portal
- IBM WebSphere Business Monitor

Traceerstellung aktivieren und Protokolle in WebSphere Portal anzeigen

Informationen zu diesem Vorgang

Die Protokolle von WebSphere Portal befinden sich im Pfad `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal`. Führen Sie zum Starten eines Trace und zur Anzeige eines Protokolls die Schritte aus, die in der Prozedur beschrieben sind.

Vorgehensweise

1. Melden Sie sich unter http://**app-host**:9060/ibm/console bei der Administrationskonsole an. Dabei steht **app-host** für den vollständig qualifizierten Hostnamen des Anwendungsservers.
2. Klicken Sie auf **Troubleshooting** > **Logs and Trace** (Fehlerbehebung > Protokolle und Trace).
3. Klicken Sie auf **WebSphere_Portal** > **Change log level details** (WebSphere Portal > Details der Protokollstufe ändern).
4. Klicken Sie auf die Registerkarte **Runtime** (Laufzeit) und fügen Sie den folgenden Befehl ein:

```
*=warning: com.ibm.iss.*=all: com.ibm.ioc.*=all
```

5. Klicken Sie auf **OK**.
6. Geben Sie die folgenden Befehle ein, um ein Protokoll anzuzeigen:

```
cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal
tail –f trace.log
```

Traceerstellung aktivieren und Protokolle für IBM WebSphere Business Monitor auf dem Anwendungsserver anzeigen

Informationen zu diesem Vorgang

Die Protokolle für IBM WebSphere Business Monitor auf dem Anwendungsserver befinden sich im Pfad `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/`. Führen Sie zum Starten eines Trace und zur Anzeige eines Protokolls die Schritte aus, die in der Prozedur beschrieben sind.

Vorgehensweise

1. Melden Sie sich unter http://**app-host**:9060/ibm/console bei der Administrationskonsole an. Dabei steht **app-host** für den vollständig qualifizierten Hostnamen des Anwendungsservers.
2. Klicken Sie auf **Troubleshooting** > **Logs and Trace** (Fehlerbehebung > Protokolle und Trace).
3. Klicken Sie auf **WBM_DE.AppTarget.WBMNode1.0** > **Change log level details** (WBM_DE.AppTarget.WBMNode1.0 > Details der Protokollstufe ändern).
4. Klicken Sie auf die Registerkarte **Runtime** (Laufzeit) und fügen Sie den folgenden Tracestufen-Code ein: `*=info: com.ibm.wbm.*=finest: com.ibm.events.*=all: com.ibm.wbimonitor.xsp.cei.*=all: com.ibm.wbimonitor.xsp.eventselector.*=all`
5. Klicken Sie auf **OK**.

Zugehörige Informationen:

Produktdokumentation zu IBM WebSphere Portal 7

Protokolldateien des Ereignisservers

Mit den folgenden Prozeduren können Sie für einige der Systeme auf dem Ereignisserver das Tracing aktivieren und Protokolle anzeigen.

Anhand der folgenden Prozeduren wird beschrieben, wie Sie für die folgenden Systeme das Tracing aktivieren und Protokolle anzeigen können:

- Tivoli Service Request Manager
- WebSphere MQ und WebSphere Message Broker
- Tivoli Netcool/OMNIbus-XML-Testmonitor
- Tivoli Netcool/OMNIbus-Datenbank (Objektserver)
- Tivoli Netcool/OMNIbus-Datenbank (Prozessagent)
- Tivoli Netcool/Impact

Tracing und Anzeigen von Protokolldateien für Tivoli Service Request Manager aktivieren

Informationen zu diesem Vorgang

Verwenden Sie die folgende Prozedur, um Fehler im Informationsfluss von Tivoli Service Request Manager an IBM Intelligent Operations Center zu beheben.

Vorgehensweise

1. Klicken Sie in der Benutzerschnittstelle von Tivoli Service Request Manager auf **Go To** > **System configuration** > **Platform Configuration** > **Logging** (Weiter mit > Systemkonfiguration > Plattformkonfiguration > Protokollierung).

2. Geben Sie unter "Root Loggers" (Rootprotokollfunktionen) im Filterfeld `integration` (Integration) ein.
3. Erweitern Sie **integration** (Integration).
4. Konfigurieren Sie die Integrationsprotokollfunktion:
   a. Klicken Sie für **Log Level** (Protokollebene) auf das Symbol **Select Value** (Wert auswählen). Klicken Sie im Fenster **Select Value** (Wert auswählen) auf **DEBUG**.
   b. Klicken Sie für **Appenders** (Appender) auf das Symbol **Manage Appenders** (Appender verwalten). Aktivieren Sie im Fenster **Manage Appenders** (Appender verwalten) das Kontrollkästchen **Dailyrolling** (Täglich rollierend) und klicken Sie anschließend auf **OK**.
   c. Aktivieren Sie das Kontrollkästchen **Active?** (Aktiv?).
   d. Klicken Sie auf das Symbol **Save Logger** (Protokollfunktion speichern).
5. Wählen Sie in der Liste **Select Action** (Aktion auswählen) den Eintrag **Set Logging Root Folder** (Protokollierungsstammordner festlegen) aus.
6. Geben Sie im Fenster **Set Logging Root Folder** (Protokollierungsstammordner festlegen) für **Root Logging Folder** (Protokollierungsstammordner) den Pfad `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1` ein und klicken Sie auf **OK**.
7. Klicken Sie auf das Symbol **Save Logger** (Protokollfunktion speichern).
8. Wählen Sie in der Liste **Select Action** (Aktion auswählen) den Eintrag **Apply Settings** (Einstellungen übernehmen) aus.
9. Geben Sie in einem Tivoli Service Request Manager-Server-Terminal die folgenden Befehle ein, um das Protokoll anzuzeigen:

   ```
   cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/maximo/logs
   tail -f ereignis_host_MXServer_maximo_scheduled.log
   ```

   ereignis_host ist der Hostname von Ereignisserver.

Zugehörige Tasks:

„Protokolldateien überprüfen" auf Seite 358
Überprüfen Sie die Tivoli Netcool/OMNIbus-Richtlinienprotokolldatei und die Tivoli Service Request Manager-Protokolldatei.

Tracing und Anzeigen von Protokolldateien für WebSphere MQ und WebSphere Message Broker aktivieren

Informationen zu diesem Vorgang

Die Protokolle für WebSphere MQ und WebSphere Message Broker werden an folgenden Positionen gespeichert:

- `/var/mqm/errors`
- `/var/mqm/qmgrs/IOC!MB!QM/errors`

Tracedateien werden in das Verzeichnis `/var/mqm/trace` geschrieben. Sie können die Traceerstellung für einen einzelnen Warteschlangenmanager oder für alle Warteschlangenmanager aktivieren, wie in der folgenden Prozedur dargestellt.

Vorgehensweise

1. Wählen Sie den entsprechenden Befehl aus, um einen Trace zu starten, zu beenden oder zu formatieren:
   - Wenn Sie einen Trace für alle Prozesse starten möchten, geben Sie folgenden Befehl ein: `strmqtrc -e`
   - Wenn Sie einen Trace für den Warteschlangenmanager des IBM Intelligent Operations Center starten möchten, geben Sie folgenden Befehl ein: `strmqtrc -m IOC.MB.QM`
   - Wenn Sie einen ausführlichen Trace für den Warteschlangenmanager des IBM Intelligent Operations Center starten möchten, geben Sie folgenden Befehl ein: `strmqtrc -t all -t detail -m IOC.MB.QM`

- Wenn Sie die gesamte Traceverarbeitung beenden möchten, geben Sie folgenden Befehl ein: `endmqtrc -a`
- Wenn Sie die binären Tracedateien im ASCII-Format formatieren möchten, geben Sie folgenden Befehl ein: `dspmqtrc *.TRC`

2. So überprüfen Sie den Status von WebSphere Message Broker:
   a. Geben Sie folgenden Befehl ein: `ps -ef | grep IOC_BROKER`
   b. Überprüfen Sie den Status der folgenden Prozesse:
      - `bipservice IOC_BROKER`
      - `bipbroker IOC_BROKER`
      - `biphttplistener IOC_BROKER`
      - `DataFlowEngine IOC_BROKER 5fe69373-2f01-0000-0080-9ab9c3579b15 default`

Tracing und Anzeigen von Protokolldateien für den Tivoli Netcool/OMNIbus-XML-Testmonitor aktivieren

Informationen zu diesem Vorgang

Die Protokolle von WebSphere Portal befinden sich in der Datei `/opt/IBM/netcool/omnibus/log/ioc_xml.log`. Führen Sie zum Starten eines Trace und zur Anzeige eines Protokolls die Schritte aus, die in der Prozedur beschrieben sind.

Vorgehensweise

1. Öffnen Sie ein Terminal auf dem Ereignisserver.
2. Geben Sie folgenden Befehl ein: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`
3. Wenn am Ende der Datei die Nachricht `Connection status OK` (Verbindungsstatus OK) nicht angezeigt wird, geben Sie folgenden Befehl ein, um die aktuelle Protokolldatei umzubenennen: `mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log`
4. Falls die Nachricht `Connection status OK` (Verbindungsstatus OK) nicht angezeigt wird, kann es außerdem vorkommen, dass die Nachricht `Probe shutting down` (Testmonitor wird gerade beendet) angezeigt wird. Geben Sie folgenden Befehl ein, um den Testmonitor erneut zu starten:
   `/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &`
5. Geben Sie nach etwa einer Minute folgenden Befehl erneut ein: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`
6. Wird die Nachricht `Connection status OK` (Verbindungsstatus OK) immer noch nicht angezeigt, überprüfen Sie die Datei `/opt/IBM/netcool/omnibus/log/ioc_xml.log` auf Fehler. Ein Verbindungsproblem kann darauf zurückzuführen sein, dass der Objektserver inaktiv ist. Lesen Sie den folgenden Abschnitt *Traceerstellung aktivieren und Protokolle für die Tivoli Netcool/OMNIbus-Datenbank (Objektserver) anzeigen*.

Tracing und Anzeigen von Protokolldateien für die Tivoli Netcool/OMNIbus-Datenbank (Objektserver) aktivieren

Informationen zu diesem Vorgang

Die Protokolldateien befinden sich an folgenden Positionen:

- `/opt/IBM/netcool/omnibus/log/ioc_xml.log`
- `/opt/IBM/netcool/omnibus/log/NCOMS*.*`. Beispiel:
  - `/opt/IBM/netcool/omnibus/log/NCOMS.log`
  - `/opt/IBM/netcool/omnibus/log/NCOMS_trigger_stats.log1`
  - `/opt/IBM/netcool/omnibus/log/NCOMS_profiler_report.log1`

Führen Sie zum Starten eines Trace und zur Anzeige eines Protokolls die Schritte aus, die in der Prozedur beschrieben sind.

Vorgehensweise

1. Melden Sie sich als Rootbenutzer bei einem Terminal an.
2. Geben Sie folgenden Befehl ein: `/opt/IBM/netcool/omnibus/bin/nco_config &`
3. Wenn Sie gefragt werden, ob Sie Daten aus `omni.dat` importieren möchten, klicken Sie auf **yes** (Ja) und klicken Sie anschließend auf **finish** (Fertigstellen).
4. Minimieren Sie das Fenster des Prozessagenten.
5. Klicken Sie mit der rechten Maustaste auf **NCOMs**.
6. Wählen Sie die geeignete Option aus:
   - Wenn die Option **Connect As...** (Verbinden als...) nicht angezeigt wird, müssen Sie den NCOMS-Objektserver starten:
     a. Zum Start des NCOMS-Objektservers müssen Sie "nco_config" schließen und folgenden Befehl eingeben: `/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &`
     b. Wenn der NCOMS-Objektserver nicht gestartet wird, suchen Sie die Datei `NCOMS.pid` im Verzeichnis `/opt/IBM/netcool/omnibus/var` und löschen Sie diese. Versuchen Sie anschließend erneut, den Server zu starten.
   - Wenn die Option **Connect As...** (Verbinden als...) angezeigt wird, klicken Sie auf **Connect As...** (Verbinden als...) und geben Sie als Benutzernamen `root` und anschließend das Kennwort ein.
7. Geben Sie nach dem Start des NCOMs-Servers folgenden Befehl ein, um den Testmonitor erneut zu starten:

   ```
   /opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
   ```

8. Geben Sie folgenden Befehl ein, um die Protokolldatei anzuzeigen: `tail -f /opt/IBM/netcool/omnibus/log/NCOMS.log`

Tivoli Netcool/OMNIbus-Datenbankprotokolldatei (Prozessagent)

Die Protokolldatei der Tivoli Netcool/OMNIbus-Datenbank (Prozessagent) befindet sich an der Position `/opt/IBM/netcool/omnibus/log/NCO_PA.log`.

Tivoli Netcool/Impact-Protokolldateien aktivieren und anzeigen

Informationen zu diesem Vorgang

Die Protokolldatei befindet sich im Pfad `opt/IBM/netcool/impact/log/`. Führen Sie zum Starten eines Trace und zur Anzeige eines Protokolls die Schritte aus, die in der Prozedur beschrieben sind.

Vorgehensweise

1. Melden Sie sich bei der Tivoli Netcool/Impact-Administrationskonsole unter `http://`*`ereignis_host`*`:9080/nci` mit dem Benutzernamen `admin` an, wobei *ereignis_host* der vollständig qualifizierte Name von Ereignisserver ist. Wenn kein Anmeldedialog angezeigt wird, geben Sie die folgenden Befehle in einem Terminalfenster ein:

   ```
   su – netcool
   /opt/IBM/netcool/bin/ewas.sh start
   ```

2. Blättern Sie im Fenster mit dem Servicestatus nach unten und vergewissern Sie sich, dass die folgenden Services ausgeführt werden. Dies ist durch ein grünes Symbol erkennbar:
   - `IOC_CAP_Event_Reader`
   - `IOC_Notification_Reader`
3. Klicken Sie im Fenster mit dem Servicestatus außerdem auf das Symbol **View Log** (Protokoll anzeigen) neben **PolicyLogger**, um zu prüfen, ob im Protokoll Fehler angezeigt werden.
4. Falls das Protokoll einen oder mehrere Fehler enthält, prüfen Sie die Protokolldateien im folgenden Verzeichnis auf weitere Details: `/opt/IBM/netcool/impact/log/`
5. Wenn Sie ausführlichere Informationen benötigen, legen Sie höhere Protokollebenen fest. Klicken Sie auf **PolicyLogger** und setzen Sie anschließend den Wert von **Highest log level** (Höchste Protokollebene) auf 3. Aktivieren Sie die gewünschten Kontrollkästchen.

Nächste Schritte

Während der Laufzeit können Sie über die Administrationskonsole von WebSphere Application Server verschiedene Protokolle aktivieren. Wenn Sie weitere Informationen zur Aktivierung der Portaltracefunktion und sonstiger Traces wünschen, die in WebSphere Portal verfügbar sind, rufen Sie den Link am Anfang des Themas auf, der Sie zur Produktdokumentation von WebSphere Portal führt. Suchen Sie dort nach *Logging and tracing* (Protokollierung und Traceerstellung).

Zugehörige Tasks:

„Protokolldateien überprüfen" auf Seite 358
Überprüfen Sie die Tivoli Netcool/OMNIbus-Richtlinienprotokolldatei und die Tivoli Service Request Manager-Protokolldatei.

MustGather-Tool bei der Installation ausführen

Es werden Protokolldateien erstellt, während IBM Intelligent Operations Center installiert wird. Es ist ein Tool verfügbar, das diese Protokolldateien zur Analyse zusammenstellt.

Vorgehensweise

1. Melden Sie sich am Installationsserver als `root`-Benutzer an und öffnen Sie ein Terminalfenster.
2. Wechseln Sie in das Verzeichnis *`Installationsausgangsverzeichnis`*`/ioc/bin`.
3. Führen Sie den Befehl **`export JAVA_HOME=/opt/ibm/java-x86_64-60/jre`** aus, um für die Verwendung von Java 6 Runtime die Variable `JAVA_HOME` einzustellen.
4. Führen Sie den Befehl **`./mustgather.sh -p`** *Kennwort* aus, wobei *Kennwort* das Topologiekennwort ist. Das Tool scannt die Datei mit den Topologieeigenschaften bei der ersten Ausführung. Wenn die Datei mit den Topologieeigenschaften nach der Ausführung des Tools geändert wird, fügen Sie **`-n`** zu dem Befehl hinzu, damit das Tool die Datei mit den Topologieeigenschaften erneut scannt. Beispiel: **`./mustgather.sh -n -p`** *Kennwort*.

Ergebnisse

Die gesammelten Protokolle und anderen Informationen werden an das Verzeichnis *`Installationsausgangsverzeichnis`*`/mustGather` auf dem Installationsserver geschrieben. Für jeden der Server ist eine Datei mit der Erweiterung `.tar` vorhanden.

Die gesammelten Informationen beinhalten Folgendes:

- Protokolle für alle Installationsphasen, u. a. Protokolle für die einzelnen auf den jeweiligen Knoten installierten Komponenten.
- Installationsprotokolle für das Tool Systemprüfung.
- Die XML-Topologiedateien.
- Alle während des Installationsprozesses verwendeten Scripts.
- Alle von Cyber Hygiene behandelten Schwachstellen.
- Die Cyber Hygiene-Scripts.

Zugehörige Konzepte:

„Tracing aktivieren und Protokolldateien anzeigen" auf Seite 311
Zur Fehlerbehebung bei Problemen im IBM Intelligent Operations Center müssen Sie möglicherweise Protokolldateien in mehreren Systemen analysieren. In den folgenden Themen erfahren Sie, wie Sie auf die Protokolldateien zugreifen können.

„Fehlersuche in den Komponenten"
Sie können das Tool "Systemprüfung" für die Suche von Komponentenfehlern im IBM Intelligent Operations Center verwenden.

Zugehörige Tasks:

„Installation der IBM Intelligent Operations Center-Architektur während einer schrittweisen Installation neu starten" auf Seite 52
Wenn die Architekturinstallation fehlschlägt, kann die Installation neu gestartet werden.

„Informationen mit IBM austauschen" auf Seite 345
Damit ein Problem diagnostiziert oder bestimmt werden kann, müssen Sie dem IBM Support möglicherweise Daten und Informationen aus Ihrem System zur Verfügung stellen. In anderen Fällen kann es hingegen vorkommen, dass Sie vom IBM Support Tools oder Dienstprogramme erhalten, die Sie zur Fehlerbestimmung heranziehen können.

Fehlersuche in den Komponenten

Sie können das Tool "Systemprüfung" für die Suche von Komponentenfehlern im IBM Intelligent Operations Center verwenden.

Über den Link am Ende des Themas erhalten Sie weitere Informationen zum Tool "Systemprüfung".

In den Tabellen der folgenden Abschnitte werden für jeden im IBM Intelligent Operations Center enthaltenen Server die Positionen der Protokolldateien aufgelistet. Alle Protokolldateien werden automatisch erstellt. Sie können diese mit den entsprechenden tail-Befehlen anzeigen.

Installationsserver

Wenn Sie Informationen zur Zusammenstellung von Installationsprotokolldateien benötigen, lesen Sie das Thema über die Ausführung des Tools "must gather". Diese Informationen können über den Link am Ende des Themas aufgerufen werden.

Anwendungsserver

Tabelle 96. Komponenten und Protokolldateien des Anwendungsservers

Komponente	Protokolldateien
IBM Cognos Administration	• /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Disp1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Disp1/SystemErr.log • /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemErr.log • Alle Protokolle im Verzeichnis /opt/IBM/cognos/c10_64/logs/
IBM HTTP Server	• /opt/IBM/HTTPServer/logs/error_log • /opt/IBM/HTTPServer/logs/access_log

Tabelle 96. Komponenten und Protokolldateien des Anwendungsservers (Forts.)

Komponente	Protokolldateien
IBM WebSphere Business Monitor	• /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log
IBM Lotus Sametime Proxy Server	• /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log
Tivoli Access Manager	• /var/pdweb/log/msg__*.log (* ist ein beliebiger Wert) • /var/pdweb/log/config_data__*.log (* ist ein beliebiger Wert)
Tivoli Access Manager WebSEAL	• /var/pdweb/log/msg__webseald-default.log • Alle Protokolle im Verzeichnis /var/pdweb/www-default/log/
Protokolle der Tivoli Directory Server-Proxy-Konfiguration	• /datahome/proxy/idsslapd-tdsproxy/logs/ibmslapd.log
WebSphere Operational Decision Management	• /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log
WebSphere Portal	• /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log • /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log
WebSphere UDDI Registry	• /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log

Datenserver

Tabelle 97. Komponenten und Protokolldateien des Datenservers

Komponente	Protokolldateien
Tivoli Directory Server	• /datahome/dsrdbm01/idsslapd- dsrdbm01/logs/ibmslapd.log • Alle Protokolle im Verzeichnis /datahome/dsrdbm01 /idsslapd- dsrdbm01/logs/

Ereignisserver

Tabelle 98. Komponenten und Protokolldateien des Ereignisservers

Komponente	Protokolldateien
Lotus Domino	• /local/notesdata/console.out • /local/notesdata/log.nsf • Alle Protokolle im Verzeichnis /local/notesdata/IBM_TECHNICAL_SUPPORT/
Lotus Sametime Community Server	Geben Sie folgenden Befehl ein, um alle relevanten Protokolldateien zu sammeln und in das Verzeichnis /local/notesdata/ zu schreiben: /local/notesdata/sh stdiagzip.sh
Tivoli Netcool/Impact	• /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log • /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log
Tivoli Netcool/OMNIbus	• /opt/IBM/netcool/log • /opt/IBM/netcool/omnibus/log
Tivoli Service Request Manager	• /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log • /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log

Verwaltungsserver

Tabelle 99. Komponenten und Protokolldateien des Verwaltungsservers

Komponente	Protokolldateien
Verwaltungsserver	• Tivoli Event Monitoring Server: /opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_ms_{nnnnnnn}.log • Tivoli Event Portal Server: /opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_cq_{nnnnnnn}.log • Embedded WebSphere Application Server-Protokolle: – Fehlerprotokoll: /opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log – Ausgabeprotokoll: /opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log – Startprotokoll: /opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/startServer.log
Tivoli Access Manager und WebSphere Portal Manager	• /var/PolicyDirector/log/msg__pdmgrd_utf8.log • /var/PolicyDirector/log/msg__pdacld_utf8.log
Tivoli Access Manager	• /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log
Tivoli Enterprise Monitoring Agent	• /opt/IBM/ITM/logs/*_*PRODUKTCODE*_{nnnnnnn}.log
Tivoli Enterprise Portal	• /opt/IBM/ITM/logs/*_*PRODUKTCODE*_{nnnnnnn}.log

Tabelle 99. Komponenten und Protokolldateien des Verwaltungsservers (Forts.)

Komponente	Protokolldateien
Tivoli Identity Manager	• /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log • /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log • Alle Protokolle in V6-Unterverzeichnissen des Verzeichnisses /var/idsldap/

Zugehörige Konzepte:

„Protokolldateien verwalten" auf Seite 275
IBM Intelligent Operations Center speichert Protokolldateien in mehreren verschiedenen Verzeichnissen. Um Probleme mit der Systemleistung zu vermeiden, müssen Sie Protokolldateien in regelmäßigen Abständen archivieren und die ursprünglichen Protokolldateien entfernen.

Zugehörige Tasks:

„MustGather-Tool bei der Installation ausführen" auf Seite 316
Es werden Protokolldateien erstellt, während IBM Intelligent Operations Center installiert wird. Es ist ein Tool verfügbar, das diese Protokolldateien zur Analyse zusammenstellt.

Zugehörige Informationen:

Verwendung des Systemprüfungstools
Das Systemprüfungstool wird zum Ermitteln des Betriebsstatus von Services verwendet, aus denen sich das IBM Intelligent Operations Center-System zusammensetzt.

IBM Support Assistant Lite installieren und verwenden

Das Tool IBM Support Assistant Lite (ISA Lite) sammelt gängige Diagnosedaten, die bei der Analyse allgemeiner Probleme hilfreich sind.

ISA Lite stellt die folgenden Arten von Informationen zusammen:

- Plattformdateien für die Fehlerbestimmung
- Systemprotokoll- und Tracedateien
- Plattformbereitstellungsdateien
- Systemkonfigurationsdateien
- Java™-Speicherauszugsdateien
- Interne Protokolldateien des Frameworks zur Fehlerbestimmung

Wenn Sie ISA Lite für IBM Intelligent Operations Center 1.5 herunterladen möchten, rufen Sie den Link am Ende des Themas auf.

Der im Downloadpaket enthaltene Leitfaden für den Schnelleinstieg enthält Anweisungen für die Installation und Verwendung von ISA Lite.

Zugehörige Informationen:

IBM Support Assistant Lite für IBM Intelligent Operations Center 1.5 herunterladen

IBM Intelligent Operations Center-Nachrichten

Jeder Abschnitt zu einer Nachricht liefert Ihnen Informationen und Empfehlungen dazu, wie Sie die Ursache einer bestimmten Fehlerbedingung im IBM Intelligent Operations Center bestimmen und welche Maßnahmen Sie ergreifen können, um den Fehler zu beheben.

Zum besseren Verständnis der Fehler, die bei der Verwendung des IBM Intelligent Operations Center auftreten können, ist jeder Abschnitt zu einer Nachricht in drei Teile untergliedert: zunächst die Nachricht, die im IBM Intelligent Operations Center angezeigt wird, oder dessen Protokolle, anschließend eine Erläuterung und eine Maßnahme.

Die Nachricht
Die Nachricht enthält zwei Kennungen: die Fehlerkennung und den zugeordneten Text. Bei der Fehlerkennung handelt es sich um die Nachrichten-ID. Es handelt sich um eine eindeutige Nummer, die eine Nachricht bezeichnet. Lautet das Schlusszeichen der Nachrichten-ID "E", handelt es sich um eine Fehlernachricht. Das Schlusszeichen "W" gibt eine Warnnachricht an und "I" eine Informationsnachricht.

Die Erläuterung
Dieser Abschnitt enthält eine ergänzende Erläuterung der Nachricht.

Die Benutzerintervention
Dieser Abschnitt enthält Empfehlungen für Korrekturmaßnahmen zur Behebung des Fehlers.

Weitere Informationen zu einer Fehlernachricht erhalten Sie, indem Sie die Nachrichten-ID der Fehlernachricht in das Suchfeld im Information Center eingeben.

Anmerkung: Die Themen in diesem Abschnitt enthalten nur Nachrichten, die spezifisch für das IBM Intelligent Operations Center sind. Informationen zu anderen Nachrichten finden Sie in der Produktdokumentation.

CIYBA0101E Die Topologiedatei {0} ist ungültig.

Erläuterung: Das Installationsprogramm hat versucht, die {0} Topologiedatei zu prüfen, und hat Fehler in der Topologiedatei festgestellt. Im Folgenden sind mögliche Fehler aufgeführt:

- Nicht alle erforderlichen Komponenten sind in der Topologiedatei enthalten.
- Grundsätzlich erforderliche Komponenten sind nicht vor abhängigen Komponenten aufgelistet.
- Komponenten, die nacheinander implementiert werden müssen, befinden sich in der Zeilengruppe für parallele Entwicklung.

Benutzeraktion: Korrigieren Sie die Topologiedatei und führen Sie die Installation erneut aus.

CIYBA0102E Die Topologie oder die Dateien mit der Topologiespezifikation wurden nicht gefunden.

Erläuterung: Jede Installationstopologie verfügt über eine zugeordnete XML-Datei und eine Spezifikation. Eine oder beide Dateien konnten nicht gefunden werden.

Benutzeraktion: Stellen Sie sicher, dass alle Installationsdateien auf dem Installationsserver extrahiert wurden. Prüfen Sie, ob die Eigenschaft `image.basedir.local` in der Datei `custom.properties` auf die richtige Position gesetzt ist. Die Datei `custom.propeties` befindet sich im Unterverzeichnis `/resource` auf dem Installationsserver, wo das Installationspaket extrahiert wurde.

CIYBA0103E Das Script {0} versucht, eine nicht vorhandene Komponente zu installieren.

Erläuterung: Das Installationsprogramm hat ein Script für eine Komponente gesucht, aber das Script wurde nicht gefunden.

Benutzeraktion: Prüfen Sie, ob der Installationsdatenträger auf dem Installationsserver extrahiert wurde. Stellen Sie sicher, dass das Basisverzeichnis in der Datei `custom.properties` korrekt konfiguriert wurde. Das Basisverzeichnis wird verwendet, um die Position des Installationsscripts abzuleiten.

CIYBA0104E Die Topologiedatei enthält ungültige Einträge.

Erläuterung: Das Installationsprogramm hat beim Lesen der Topologiedatei und beim Erstellen der implementierbaren Einheiten für die jeweiligen Komponenten einen Fehler festgestellt. Dies ist normalerweise ein interner Fehler, es sei denn, es wird eine benutzerdefinierte Topologie installiert.

Möglicherweise ist die Topologiedatei beschädigt oder nicht ordnungsgemäß angegeben.

Benutzeraktion: Prüfen Sie die Topologiedatei auf folgende Fehler:

- Doppelt vorhandene Komponenten-IDs.
- Fehlende Komponenten-IDs oder Typattribute.
- Spezifikation eines Verbindungsattributs, die über keine übergeordnete Komponente verfügt.
- Validierung des XML-Schemas für die Topologie schlägt fehl.

CIYBA0105E Die Datei {0} wurde nicht gefunden.

Erläuterung: Das Installationsprogramm konnte die Datei {0} nicht finden.

Benutzeraktion: Stellen Sie sicher, dass alle Installationsdateien auf dem Installationsserver extrahiert wurden. Prüfen Sie, ob die Eigenschaft `image.basedir.local` in der Datei `custom.properties` auf die Position zur Erfassung gesetzt ist. Die Datei `custom.properties` befindet sich im Unterverzeichnis `/resource` auf dem Installationsserver, wo das Installationspaket extrahiert wurde.

CIYBA0106E Die Datei {0} konnte nicht gespeichert werden.

Erläuterung: Das Installationsprogramm hat versucht, die Datei mit dem Namen {0} zu schreiben, und es wurde ein E/A-Dateifehler zurückgegeben.

Benutzeraktion: Prüfen Sie, ob auf die angegebene Position mit der Benutzer-ID des Installationsprogramms zugegriffen werden kann. Stellen Sie sicher, dass genügend Speicherplatz auf dem Datenträger vorhanden ist und dass die Partition nicht beschädigt ist.

CIYBA0107E Eigenschaftsverweis {0} wurde in der Topologiedatei {1} nicht gefunden

Erläuterung: Während der Installation sind für einige Komponenten Eigenschaftswerte aus den Softwarevoraussetzungen erforderlich. Diese Komponenten verwenden Eigenschaftsverweise in der Topologiedatei, um die erforderlichen Eigenschaftswerte zu bestimmen. Der Eigenschaftsverweis konnte in der Topologiedatei nicht gefunden werden.

Benutzeraktion: Die Topologiedatei ist beschädigt. Dies ist möglicherweise auf manuelle Bearbeitungsvorgänge mit ungültigen Eingaben zurückzuführen oder darauf, dass die Installation keine Topologiedatei mit korrekten Werten geschrieben hat. Bestimmen Sie, welche Komponenten nicht ordnungsgemäß installiert wurden. Entfernen Sie alle nicht ordnungsgemäß installierten Komponenten, korrigieren Sie die Topologiedatei und führen Sie eine Neuinstallation durch.

CIYBA0108E Komponente {0} wurde in der Topologiedatei {1} nicht gefunden

Erläuterung: Das Installationsprogramm hat die Komponenten-ID {0} in der Topologiedatei {1} erwartet. Die Komponenten-ID wurde nicht gefunden. Der Fehler ist möglicherweise auf eine nicht ordnungsgemäß angegebene Abhängigkeit in einem Verbindungselement einer anderen Komponente zurückzuführen.

Benutzeraktion: Prüfen Sie die Topologiedatei auf Verweise auf {0}. Korrigieren Sie nicht korrekte Verbindungselemente für die Komponente {0} und führen Sie die Installation erneut durch.

CIYBA0109E Eigenschaft {0}.{1} in Topologiedatei {2} ist ungültig.

Erläuterung: Die Eigenschaft wurde in der Topologiedatei bzw. in einer Datei mit Spezifikationseigenschaften nicht gefunden.

Benutzeraktion: Wenn die Eigenschaft fehlt, fügen Sie sie der Datei mit den Spezifikationseigenschaften oder der Topologiedatei hinzu. Dieser Fehler ist möglicherweise auch auf eine falsche Schreibweise der Eigenschaft zurückzuführen. Korrigieren Sie die Topologiedatei oder die Datei mit den Spezifikationseigenschaften und führen Sie die Installation erneut durch.

CIYBA0110E Die Eigenschaft {0}.{1} in Topologiedatei {2} kann nicht gefunden werden.

Erläuterung: Eine implementierbare Einheit verweist auf eine weitere, über Rolle {1} angegebene Einheit. Entweder wird die abhängige implementierbar Einheit nicht gefunden oder die Rollen stimmen nicht überein.

Benutzeraktion: Die angegebene Topologiedatei enthält Verweise auf die angezeigte Eigenschaft, jedoch kann die Definition dieser Eigenschaft nicht in der Topologiedatei gefunden werden. Diese Situation kann auftreten, wenn die Topologiedatei manuell bearbeitet wurde und eine Komponente entfernt wurde, jedoch die Verweise auf diese Komponente immer noch bestehen.

CIYBA0111E Master-Host für Komponente {0} kann nicht abgerufen werden.

Erläuterung: Eine Topologiekomponente muss einem Zielhost zugeordnet sein. Eine verwaiste Topologiekomponente ist angegeben.

Benutzeraktion: Prüfen Sie die Topologiekomponente {0} und stellen Sie sicher, dass sie über eine Folge von Verbindungsattributen verfügt, die zuletzt eine Komponente mit einem Hostattribut aufweist.

CIYBA0112E Topologiedatei {0} konnte nicht gelesen werden

Erläuterung: Das Installationsprogramm konnte die angegebene Topologiedatei nicht lesen.

Benutzeraktion: Prüfen Sie, ob sich die angegebene Topologiedatei im Installationsverzeichnis befindet und ob das Installationsprogramm Zugriff auf das Verzeichnis hat.

CIYBA0113E Datei {0} konnte nicht gespeichert werden.

Erläuterung: Das Installationsprogramm konnte die angegebene Datei nicht speichern.

Benutzeraktion: Prüfen Sie, ob das Installationsprogramm Zugriff auf das Installationsverzeichnis hat.

CIYBA0114E Die Eigenschaft {0}.{1} kann nicht gesetzt werden.

Erläuterung: Das Installationsprogramm konnte die angegebene Eigenschaft nicht aktualisieren.

Benutzeraktion: Die Topologiedatei ist entweder beschädigt oder sie wurde manuell bearbeitet und es wurden ungültige Eigenschaftswerte eingefügt. Korrigieren Sie die Topologiedatei und führen Sie die Installation erneut aus.

CIYBA0115E Die Topologiedatei {0} kann nicht gefunden werden.

Erläuterung: Das Installationsprogramm konnte auf die angegebene Topologiedatei nicht zugreifen.

Benutzeraktion: Prüfen Sie, ob sich die Topologiedatei im vom Installationsprogramm angegebenen Verzeichnis befindet, und stellen Sie sicher, dass das Installationsprogramm Zugriff auf das Verzeichnis hat.

CIYBA0116E Es kann nicht an die Eigenschaftendatei {0} geschrieben werden.

Erläuterung: Das Installationsprogramm konnte nicht an die angegebene Eigenschaftendatei schreiben.

Benutzeraktion: Prüfen Sie, ob die vom Installationsprogramm verwendete Benutzer-ID Zugriff auf die temporären Verzeichnisse auf den Zielservern hat. Das Verzeichnis auf den Zielservern, in das die temporären Installationsscripts geschrieben werden, wird über die Eigenschaft `Unix.script.basedir.remote` in der Datei `custom.properties` angegeben. Korrigieren Sie diesen Eigenschaftswert, wenn er nicht ordnungsgemäß angegeben ist.

CIYBA0117E Das Installationsprogramm konnte den Schlüsselspeicher nicht erstellen.

Erläuterung: Das Installationsprogramm konnte den Schlüsselspeicher nicht erstellen.

Benutzeraktion: Prüfen Sie, ob die vom Installationsprogramm verwendete Benutzer-ID Zugriff auf alle Unterverzeichnisse hat, in denen die Installationsmedien extrahiert wurden.

CIYBA0118E Das Installationsprogramm konnte mit dem bereitgestellten Kennwort nicht auf den Schlüsselspeicher zugreifen. Das Kennwort ist falsch oder der Schlüsselspeicher ist beschädigt.

Erläuterung: Das Installationsprogramm konnte nicht auf den Schlüsselspeicher zugreifen.

Benutzeraktion: Prüfen Sie, ob das bereitgestellte Kennwort korrekt ist, und stellen Sie sicher, dass der Schlüsselspeicher nicht beschädigt ist. Generieren Sie den Schlüsselspeicher mit einem neuen Kennwort erneut, indem Sie die Lösung neu installieren.

CIYBA0119E Eigenschaft {0} in Topologiedatei {1} konnte nicht verschlüsselt werden.

Erläuterung: Das Installationsprogramm konnte die angegebene Eigenschaft mit dem in der Topologiedatei bereitgestellten Kennwort nicht verschlüsseln.

Benutzeraktion: Stellen Sie sicher, dass der Schlüsselspeicher nicht beschädigt ist und dass das Kennwort für die Topologie korrekt ist. Gegebenenfalls müssen Sie den Schlüsselspeicher mit einem neuen Kennwort erneut erstellen, indem Sie eine Neuinstallation durchführen.

CIYBA0120E Eigenschaft {0} in Topologiedatei {1} konnte nicht entschlüsselt werden.

Erläuterung: Ein Versuch, die angegebene Eigenschaft zu lesen und zu entschlüsseln, ist fehlgeschlagen.

Benutzeraktion: Prüfen Sie, ob die vom Installationsprogramm verwendete Benutzer-ID Zugriff auf die angegebene Topologiedatei hat, und stellen Sie sicher, dass sich die Topologiedatei im erwarteten Verzeichnis befindet. Prüfen Sie, ob das Kennwort und der geheime Schlüssel korrekt sind. Führen Sie die Installation erneut aus.

CIYBA0121E Die Schlüsselspeicherdatei {0} ist bereits vorhanden.

Erläuterung: Dieser Fehler sollte mit der IBM Installation Manager-Installation nicht auftreten. IBM Installation Manager steuert den Installationsfluss und stellt sicher, dass kein Versuch unternommen wird, den Schlüsselspeicher neu zu generieren.

Benutzeraktion: Prüfen Sie, ob die Installation nicht bereits ausgeführt wurde. Führen Sie das Installationsprogramm erneut aus, wenn der vorhandene Schlüsselspeicher aus einem vorherigen Installationsversuch entfernt wurde.

CIYBA0122E Der Schlüsselspeicher für die Topologie ist nicht vorhanden. Führen Sie den Befehl "createSecretKey" aus.

Erläuterung: Dieser Fehler sollte nicht auftreten, wenn Sie die IBM Installation Manager-Installation ausführen. Die IBM Installation Manager-Installation akzeptiert den geheimen Schlüssel automatisch und generiert den Schlüsselspeicher.

Benutzeraktion: Wenn Sie eine schrittweise Installation ausführen, führen Sie die Schritte zum Generieren eines Schlüsselspeichers aus.

CIYBA0123E Die Topologie {0} ist nicht vollständig installiert.

Erläuterung: Das Installationsprogramm hat festgestellt, dass nicht alle Komponenten in der Topologie installiert wurden.

Benutzeraktion: Prüfen Sie die Topologiedatei und bestimmen Sie die Komponenten, die nicht installiert wurden. Starten Sie die Installation neu.

CIYBA0124E Die Eigenschaftendatei {0} kann nicht gefunden werden.

Erläuterung: Das Installationsprogramm hat versucht, die angegebene Eigenschaftendatei zu lesen. Die Datei konnte jedoch nicht gefunden werden.

Benutzeraktion: Stellen Sie sicher, dass die Eigenschaften aus dem Installationspaket extrahiert wurden. Prüfen Sie, ob die vom Installationsprogramm verwendete Benutzer-ID Zugriff auf alle Verzeichnisse hat, in denen das Paket extrahiert wurde.

CIYBA0125E Es kann nicht an die Eigenschaftendatei {0} geschrieben werden

Erläuterung: Das Installationsprogramm hat versucht, eine Datei mit Laufzeitvariablenwerten zu aktualisieren, und es wurde eine E/A-Ausnahme zurückgegeben.

Benutzeraktion: Prüfen Sie, ob auf die angegebene Position mit der Benutzer-ID des Installationsprogramms zugegriffen werden kann. Prüfen, Sie ob genügend Speicherplatz im Dateisystem zur Verfügung steht, und stellen Sie sicher, dass die Plattenpartition nicht beschädigt ist.

CIYBA0126E Der Wert für Eigenschaft {0} aus Topologiedatei {1} kann nicht festgelegt werden

Erläuterung: Das Installationsprogramm konnte den angegebenen Eigenschaftswert nicht lesen.

Benutzeraktion: Prüfen Sie, ob die Eigenschaft in der angegebenen Topologie die korrekte XML-Syntax aufweist. Stellen Sie sicher, dass die Topologiedatei nicht beschädigt oder fehlerhaft ist. Entfernen Sie alle Sonderzeichen aus der Datei und starten Sie die Installation neu.

CIYBA0127E Die Spezifikationsdatei {0} der Lösung kann nicht gelesen werden

Erläuterung: Das Installationsprogramm hat versucht, die angegebene Datei zu lesen, und es wurde ein E/A-Dateifehler zurückgegeben.

Benutzeraktion: Stellen Sie sicher, dass die Datei im angegebenen Verzeichnis vorhanden ist. Prüfen Sie, ob die vom Installationsprogramm verwendete Benutzer-ID Zugriff auf alle Verzeichnisse hat, in denen das Paket extrahiert wurde.

CIYBA0128E Die Datei {0} konnte nicht gespeichert werden.

Erläuterung: Das Installationsprogramm hat versucht, die angegebene Datei zu schreiben, und es wurde ein E/A-Fehler zurückgegeben.

Benutzeraktion: Prüfen Sie, ob auf die angegebene Position mit der Benutzer-ID des Installationsprogramms zugegriffen werden kann. Prüfen, Sie ob genügend Speicherplatz im Dateisystem zur Verfügung steht, und stellen Sie sicher, dass die Plattenpartition nicht beschädigt ist.

CIYBA0129E Die Lösungspaketdatei {0} kann nicht gelesen werden.

Erläuterung: Das Installationsprogramm hat versucht, die angegebene Datei zu lesen, und es wurde ein E/A-Dateifehler zurückgegeben.

Benutzeraktion: Stellen Sie sicher, dass die Datei im angegebenen Verzeichnis vorhanden ist. Prüfen Sie, ob die vom Installationsprogramm verwendete Benutzer-ID Zugriff auf alle Verzeichnisse hat, in denen das Paket extrahiert wurde.

CIYBA0130E Die Lösungspaketdatei {0} ist nicht vorhanden.

Erläuterung: Das Installationsprogramm hat versucht, die angegebene Datei zu lesen, und es wurde ein E/A-Dateifehler zurückgegeben.

Benutzeraktion: Prüfen Sie die Berechtigungen der in der Nachricht angegebenen Datei. Stellen Sie sicher, dass die vom Installationsprogramm verwendete Benut-

zer-ID über Berechtigungen zum Lesen der Datei verfügt. Ändern Sie bei Bedarf die Dateiberechtigungen.

CIYBA0131E Das Installationsprogramm konnte die Topologiedatei {0} nicht laden. Die E/A-Dateinachricht war {1}.

Erläuterung: Der angegebene Fehler wurde beim Versuch, die angegebene Topologiedatei zu importieren, zurückgegeben.

Benutzeraktion: Prüfen Sie, ob sich die angegebene Topologiedatei im korrekten Verzeichnis befindet. Stellen Sie sicher, dass die Topologiedatei keine ungültigen Zeichen enthält. Stellen Sie sicher, dass das Installationsprogramm auf das Verzeichnis mit der Topologiedatei zugreifen kann.

CIYBA0140E Zugriff auf die erforderlichen Installationsdateien nicht möglich.

Erläuterung: Das Installationsprogramm konnte eine erforderliche Datei nicht lesen.

Benutzeraktion: Prüfen Sie, ob auf die Position, an der das Installationspaket extrahiert wurde, mit der Benutzer-ID des Installationsprogramms zugegriffen werden kann. Stellen Sie sicher, dass die Plattenpartition nicht beschädigt ist. Extrahieren Sie das Installationspaket erneut und wiederholen Sie die Installation.

CIYBA0141E Installationsdatei {0} wurde nicht gefunden.

Erläuterung: Das Installationsprogramm hat versucht, die angegebene Datei zu lesen, und es wurde ein E/A-Dateifehler zurückgegeben.

Benutzeraktion: Stellen Sie sicher, dass die Datei im angegebenen Verzeichnis vorhanden ist. Prüfen Sie, ob die vom Installationsprogramm verwendete Benutzer-ID Zugriff auf alle Verzeichnisse mit dem extrahierten Installationspaket hat.

CIYBA0142E Es kann nicht an Installationsdatei {0} geschrieben werden.

Erläuterung: Das Installationsprogramm hat versucht, in die angegebene Datei zu schreiben, und es wurde ein E/A-Dateifehler zurückgegeben.

Benutzeraktion: Prüfen Sie, ob die vom Installationsprogramm verwendete Benutzer-ID Zugriff auf alle Verzeichnisse mit dem extrahierten Installationspaket hat. Stellen Sie sicher, dass die Plattenpartition nicht beschädigt ist und dass genügend Speicherplatz vorhanden ist.

CIYBA0143E Das Installationsprogramm konnte die Topologiedatei nicht verarbeiten.

Erläuterung: Das Installationsprogramm liest die Topologiedatei und generiert temporäre Dateien mit Laufzeitwerten. Das Installationsprogramm hat beim Verarbeiten der Topologiedatei und beim Schreiben der temporären Dateien einen Fehler festgestellt. Dieser Fehler ist höchstwahrscheinlich auf E/A-Dateifehler zurückzuführen.

Benutzeraktion: Prüfen Sie, ob die vom Installationsprogramm verwendete Benutzer-ID Zugriff auf alle Verzeichnisse hat, in denen das Installationspaket extrahiert wurde. Stellen Sie sicher, dass die Plattenpartition nicht beschädigt ist und dass genügend Speicherplatz vorhanden ist.

CIYBA0150E Die Spezifikationsdatei {0} der Topologie kann nicht gelesen werden.

Erläuterung: Das Installationsprogramm hat versucht, die angegebene Datei zu lesen, und es wurde ein E/A-Dateifehler zurückgegeben.

Benutzeraktion: Stellen Sie sicher, dass die Datei im angegebenen Verzeichnis vorhanden ist. Prüfen Sie, ob die vom Installationsprogramm verwendete Benutzer-ID Zugriff auf alle Verzeichnisse hat, in denen das Installationspaket extrahiert wurde.

CIYBA0160E Die Regelspezifikationsdatei wurde im Verzeichnis {0} nicht gefunden.

Erläuterung: Das Installationsprogramm konnte die Datei `rule-spec.xml`, die die Regeln zur Vorabprüfung definiert, nicht laden.

Benutzeraktion: Stellen Sie sicher, dass das angegebene Verzeichnis vorhanden ist. Stellen Sie zudem sicher, dass auf das angegebene Verzeichnis mit der Benutzer-ID des Installationsprogramms zugegriffen werden kann.

CIYBA0161E Der Regelname {0} ist ungültig.

Erläuterung: Das Installationsprogramm hat einen falschen Regelnamen in der Datei `rule-spec.xml` bestimmt. Diese Datei definiert die Regeln, die vom Schritt zur Vorabprüfung verwendet werden.

Benutzeraktion: Stellen Sie sicher, dass der Regelname in der Datei `rule-spec.xml` korrekt ist. Den korrekten Regelnamen finden Sie in einer nicht geänderten Version der Datei `rule-spec.xml`.

CIYBA0162E Prüfung der Installationsvoraussetzungen ist für Topologie {0} fehlgeschlagen.

Erläuterung: Der Schritt zur Vorabprüfung ist fehlgeschlagen, da mindestens ein Konfigurationsziel die Voraussetzungen des unterstützten Systems nicht erfüllt hat.

Benutzeraktion: Stellen Sie sicher, dass die geplante Topologie die unterstützten Mindestvoraussetzungen erfüllt.

CIYBA0163W Der Betriebssystemtyp des Zielservers {0} ist nicht {1}.

Erläuterung: Der Schritt zur Vorabprüfung hat ein nicht unterstütztes Betriebssystem auf dem angegebenen Zielserver erkannt.

Benutzeraktion: Stellen Sie sicher, dass das Betriebssystem auf dem Zielserver die Voraussetzungen des unterstützten Systems erfüllt.

CIYBA0164W Es wurde erwartet, dass der Server {0} über ein {1}-Bit-Betriebssystem verfügt.

Erläuterung: Der Schritt zur Vorabprüfung hat ein falsches Betriebssystem auf dem Zielserver erkannt.

Benutzeraktion: Stellen Sie sicher, dass der Betriebssystemtyp auf dem Zielserver die Systemvoraussetzungen erfüllt.

CIYBA0165W CPU des Zielservers {0} ist keine x86- oder s390-CPU (64-Bit).

Erläuterung: Der Schritt zur Vorabprüfung hat einen nicht unterstützten CPU-Typ für den angegebenen Zielserver erkannt.

Benutzeraktion: Stellen Sie sicher, dass der CPU-Typ für den Zielserver die Systemvoraussetzungen erfüllt.

CIYBA0166E Verbindung zum Zielserver {0} nicht möglich.

Erläuterung: Das Installationsprogramm konnte bei Ausführung des Schritts zur Vorabprüfung keine Verbindung zum fernen Server herstellen.

Benutzeraktion: Prüfen Sie, ob zwischen dem Installationsserver und den Zielservern eine funktionsfähige Verbindung besteht. Prüfen Sie Vorabprüfungsprotokolle auf andere Fehler.

CIYBA0167E Verbindung zum Server {0} aufgrund eines falsch angegebenen Hostnamens, Kontos oder Kennworts nicht möglich.

Erläuterung: Das Installationsprogramm konnte den Schritt zur Vorabprüfung nicht ausführen. Das Installationsprogramm konnte keine Verbindung zum Zielserver herstellen.

Benutzeraktion: Stellen Sie sicher, dass der Hostname das korrekte Format aufweist und dass die Anmeldedetails für den fernen Server korrekt sind. Prüfen Sie Vorabprüfungsprotokolle auf zusätzliche Informationen.

CIYBA0168E Die Zeit oder Zeitzone für Server {0} und {0} ist nicht synchronisiert.

Erläuterung: Es gibt einen Unterschied zwischen der für die Server festgelegten Zeit oder Zeitzone.

Benutzeraktion: Stellen Sie sicher, dass die Zeit und die Zeitzone für alle Server identisch sind.

CIYBA0169W Betriebssystemtyp und CPU-Architektur auf Server {0} prüfen

Erläuterung: Der Schritt des Installationsprogramms zur Vorabprüfung hat ein nicht unterstütztes Betriebssystem und eine nicht unterstützte CPU-Architektur für einen Zielserver gefunden.

Benutzeraktion: Stellen Sie sicher, dass alle Server die Systemvoraussetzungen für die Lösung erfüllen.

CIYBA0170W Zeitzone sowie Datum und Uhrzeit auf allen Servern prüfen

Erläuterung: Auf diese Nachricht folgt das Wort "pass" oder "fail". Das Wort, das auf die Nachricht folgt, bestimmt die zu ergreifende Maßnahme.

Benutzeraktion: Wenn auf die Nachricht "pass" folgt, ist keine Reaktion erforderlich. Wenn auf die Nachricht "fail" folgt, müssen die Server synchronisiert werden. Die Systemparameter für Zeitzone, Datum und Uhrzeit müssen auf allen Knoten in der Topologie identisch sein.

CIYBA0171I Prüfung der Installationsvoraussetzungen startet mit der Verwendung der Instanz {0}.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0172I Prüfung der Installationsvoraussetzungen wurde erfolgreich beendet.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0173I Prüfung der Installationsvoraussetzungen wurde mit {0} Warnungen und {1} Fehlern beendet:

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0176E Die Anmeldedaten für Server {0} sind falsch. Prüfen Sie die Benutzer-ID und das Kennwort für den Server.

Erläuterung: Der Schritt des Installationsprogramms zur Vorabprüfung hat falsche Anmeldedaten für den Zielserver gefunden.

Benutzeraktion: Prüfen Sie, ob die Kontodetails für den Server die korrekte Benutzer-ID und das korrekte Kennwort enthalten.

CIYBA0177W Verbindung zum fernen Server nicht möglich. Es wird auf Neuversuch gewartet.

Erläuterung: Der Schritt des Installationsprogramms zur Vorabprüfung konnte keine Verbindung zum fernen Server ausführen. Es wird erneut versucht, eine Verbindung herzustellen.

Benutzeraktion: Es ist keine Maßnahme erforderlich. Die Wartezeit des Installationsprogramms wird über die Eigenschaft `waiting.time` in der Datei `custom.properties` festgelegt. Nach Ablauf der Wartezeit wird erneut versucht, eine Verbindung herzustellen.

CIYBA0178W Verbindung mit {0} nicht möglich, {1} Millisekunden bis zum nächsten Verbindungsversuch warten.

Erläuterung: Es bestehen Verbindungsprobleme im System.

Benutzeraktion: Wenn mehrere Verbindungsversuche fehlschlagen, wenden Sie sich an den Netzadministrator, damit dieser die Verbindungsprobleme löst, und wiederholen Sie die Installation.

CIYBA0179E Es wurden keine Werte für Schlüssel {0} in der Eigenschaftendatei der Topologie bereitgestellt.

Erläuterung: Der Schritt des Installationsprogramms zur Vorabprüfung konnte keine Werte für den Hostnamen, den Benutzernamen oder das Kennwort aus der Eigenschaftendatei abrufen.

Benutzeraktion: Stellen Sie sicher, dass der Hostname, der Benutzername und das Kennwort in der Eigenschaftendatei korrekt angegeben sind.

CIYBA0180E Die für Server {0} eingegebene Benutzer-ID hat keine Rootberechtigungen.

Erläuterung: Der Schritt des Installationsprogramms zur Vorabprüfung hat festgestellt, dass das für den angegebenen Server verwendete Konto keine Rootberechtigungen hat.

Benutzeraktion: Ändern Sie die für den Server verwendete Benutzer-ID in eine Benutzer-ID mit Rootberechtigungen oder fügen Sie der für den Server angegebenen Benutzer-ID Rootberechtigungen hinzu.

CIYBA0181E Prüfen Sie die Rootbenutzer-ID und das Kennwort für Server {0}.

Erläuterung: Der Schritt des Installationsprogramms zur Vorabprüfung hat festgestellt, dass die Zugriffsberechtigungen der für den Server verwendeten Benutzer-ID nicht ausreichen.

Benutzeraktion: Prüfen Sie, ob die Zugriffsberechtigungen des Kontos ausreichen.

CIYBA0182E Konnektivität zwischen Installationsserver und {0} prüfen

Erläuterung: Der Schritt des Installationsprogramms zur Vorabprüfung konnte keine Verbindung zwischen dem Installationsserver und dem Zielserver herstellen.

Benutzeraktion: Prüfen Sie die Konnektivität zwischen Servern. Prüfen Sie Vorabprüfungsprotokolle auf zusätzliche Informationen.

CIYBA0183E Wert {0} für Schlüssel {1} ist ungültig, er muss "EM64T", "AMD64" oder "S390" lauten.

Erläuterung: Der Schlüsselwert sollte einem der angegebenen Werte entsprechen.

Benutzeraktion: Korrigieren Sie den Wert und führen Sie die Installation erneut aus.

CIYBA0184E Wert {0} für Schlüssel {1} ist kein gültiger Hostname

Erläuterung: Der Schritt des Installationsprogramms zur Vorabprüfung hat festgestellt, dass der bereitgestellte Wert kein gültiger Hostname ist.

Benutzeraktion: Stellen Sie sicher, dass der Hostname das korrekte Format und einen korrekten Wert aufweist.

CIYBA0185E Prüfung der Installationsvoraussetzungen ist für Regel {0} fehlgeschlagen

Erläuterung: Der Schritt des Installationsprogramms zur Vorabprüfung konnte die angegebene Regel nicht prüfen.

Benutzeraktion: Prüfen Sie Vorabprüfungsprotokolle auf zusätzliche Nachrichten. Korrigieren Sie den Fehler und führen Sie die Installation erneut aus.

CIYBA0187E SSH-Schlüsselspeicher "{0}" wurde angegeben, der Zugriff darauf war jedoch nicht möglich. Zertifikatbasiertes SSH-Protokoll ist nicht verfügbar. Details: {1}.

Erläuterung: Der Schritt des Installationsprogramms

zur Vorabprüfung hat bei der Herstellung einer Verbindung zum Zielserver ungültige Daten im SSH-Schlüsselspeicher gefunden.

Benutzeraktion: Prüfen Sie die Details in der Nachricht und prüfen Sie, ob der bereitgestellte Schlüsselspeicher über entsprechende Einträge verfügt.

CIYBA0190E Die Komponente {0} muss vor der Komponente {1} in der Topologiedatei erscheinen.

Erläuterung: Die Topologiedatei wurde nicht ordnungsgemäß geändert. Eine vorausgesetzte Komponente erscheint nach einer abhängigen Komponente.

Benutzeraktion: Ändern Sie die Topologiedatei, sodass Komponenten, die über Abhängigkeiten verfügen, nach den Komponenten erscheinen, von denen sie abhängig sind.

CIYBA0191E Es gibt eine Abhängigkeit zwischen Komponente {0} und Komponente {1} in der Topologiedatei. Die Komponenten können nicht parallel implementiert werden.

Erläuterung: Die Komponenten können nicht parallel implementiert werden, wenn eine Abhängigkeit zwischen ihnen besteht. Beispiel: Wenn Komponente 2 eine Voraussetzung von Komponente 1 ist.

Benutzeraktion: Entfernen Sie die Komponenten aus der parallelen Zeilengruppe der Topologiedatei.

CIYBA0192E Die Eigenschaft {1}.{2} weist einen ungültigen Referenzwert {0} in der Topologiedatei auf.

Erläuterung: Der in der Nachricht enthaltene Referenzwert ist für die angegebene Eigenschaft nicht gültig.

Benutzeraktion: Verwenden Sie das ID-Feld, um die Eigenschaftsdefinition zu lokalisieren, und stellen Sie sicher, dass alle Verweise auf die Eigenschaft den korrekten Wert aufweisen.

CIYBA0193E Für die Komponente {0} wurden doppelt vorhandene Verbindungen {1} in der Topologiedatei identifiziert.

Erläuterung: Es sind doppelt vorhandene Verbindungen für die Komponente in der Topologiedatei definiert.

Benutzeraktion: Entfernen Sie die doppelt vorhandenen Verbindungsinformationen in der Topologiedatei und führen Sie das Installationsprogramm erneut aus.

CIYBA0194E Die Eigenschaft {0} ist in Komponente {0} doppelt vorhanden

Erläuterung: Für die Komponente ist eine doppelt vorhandene Eigenschaft definiert.

Benutzeraktion: Entfernen Sie die doppelt vorhandene Eigenschaft für die Komponente in der Eigenschaftendatei.

CIYBA0195E Die Komponente {0} in der Topologiedatei weist eine ungültige Eigenschaft auf: {0}.

Erläuterung: Die angegebene Eigenschaft wurde für die angegebene Komponente nicht erwartet. Die Ursache hierfür ist möglicherweise eine falsch geschriebene Eigenschaft oder eine Eigenschaft, die in der Eigenschaftsspezifikation fehlt.

Benutzeraktion: Fügen Sie die spezifizierte Eigenschaft der Eigenschaftendatei oder der Topologie hinzu. Wenn die Eigenschaft eine falsche Schreibweise aufweist, korrigieren Sie sie. Korrigieren Sie die Topologiedatei oder die Eigenschaftsspezifikationsdatei, und starten Sie die Installation neu.

CIYBA0196E In Komponente {1} fehlt die Eigenschaft {0}

Erläuterung: Die Komponente muss die angegebene Eigenschaft aufweisen.Der Fehler ist möglicherweise auf eine falsch geschriebene Eigenschaft oder auf eine in der Eigenschaftsspezifikationsdatei fehlende Eigenschaft zurückzuführen.

Benutzeraktion: Fügen Sie die Eigenschaft der Spezifikationseigenschaftendatei oder der Topologie hinzu. Wenn der Fehler auf eine falsche Schreibweise zurückzuführen ist, korrigieren Sie ihn. Starten Sie die Installation neu.

CIYBA0197E Für Komponente {1} wurde ein ungültiger Komponententyp {1} angegeben.

Erläuterung: Für die Komponente wurde ein ungültiger Komponententyp angegeben.

Benutzeraktion: Prüfen Sie, ob die Spezifikationsdatei für die Komponenten den Komponententyp enthält. Komponentenspezifikationsdateien befinden sich im Unterverzeichnis *Installationsausgangsverzeichnis*/spec/*Komponente* auf dem Installationsserver.

CIYBA0198E Die Verbindung {0} ist für Komponente {1} ungültig

Erläuterung: Die definierte Verbindung ist für die Komponente ungültig.

Benutzeraktion: Prüfen Sie die Schreibweise der Verbindung in der Topologiedatei für die Komponente und stellen Sie sicher, dass sie korrekt ist.

CIYBA0199E Die Verbindung {0} fehlt in der Komponente {1}.

Erläuterung: Es ist keine Verbindung für die angegebene Komponente definiert.

Benutzeraktion: Prüfen Sie die Spezifikationsdatei der Komponente und stellen Sie sicher, dass die Verbindungsinformationen enthalten sind.

CIYBA0200E Die Verbindungsinformationen für {0} sind nicht vorhanden.

Erläuterung: Die Verbindungs-ID ist für die angegebene Komponente nicht vorhanden.

Benutzeraktion: Prüfen Sie, ob die Verbindungs-ID in der Topologiedatei angegeben ist. Prüfen Sie, ob die Schreibweise der Verbindungs-ID korrekt ist und ob die Verbindungs-ID auf eine Zeilengruppe in der Topologiedatei verweist, die die zugehörige Komponente für die Verbindungs-ID definiert.

CIYBA0201E Verbindung zum fernen Server {0} nicht möglich.

Erläuterung: Das Installationsprogramm hat ein Konnektivitätsproblem für den angegebenen Server festgestellt.

Benutzeraktion: Prüfen Sie, ob Verbindungsprobleme zwischen den Servern bestehen. Führen Sie den Schritt des Installationsprogramms zur Vorabprüfung aus und lösen Sie etwaige Konnektivitätsprobleme.

CIYBA0202E Benutzername oder Kennwort ist für Server {0} ungültig.

Erläuterung: Das Installationsprogramm hat ungültige Berechtigungsnachweise für den angegebenen Server gefunden.

Benutzeraktion: Prüfen Sie, ob die Serverberechtigungsnachweise in der Topologiedatei korrekt sind.

CIYBA0203E Datei {0} ist nicht vorhanden.

Erläuterung: Bei einem Versuch, die Eigenschaftendatei zu laden, wurde ein Fehler zurückgegeben.

Benutzeraktion: Prüfen Sie, ob der Pfad zur Eigenschaftendatei korrekt ist, und stellen Sie sicher, dass die Datei vorhanden ist.

CIYBA0204E Datei {0} kann nicht gelesen/geschrieben werden.

Erläuterung: Das Installationsprogramm hat versucht, die Eigenschaftendatei zu lesen, und es wurde ein Fehler zurückgegeben.

Benutzeraktion: Stellen Sie sicher, dass der Pfad zur Eigenschaftendatei korrekt ist und dass die angegebene Datei vorhanden ist.

CIYBA0205E Verzeichnis {0} auf {1} kann nicht erstellt werden.

Erläuterung: Das Installationsprogramm konnte kein Verzeichnis auf dem fernen Server erstellen.

Benutzeraktion: Stellen Sie sicher, dass auf dem fernen Server ausreichend Speicherplatz vorhanden ist und dass die vom Installationsprogramm verwendete Benutzer-ID über die entsprechenden Zugriffsrechte und Berechtigungen zum Erstellen eines Verzeichnisses verfügt.

CIYBA0206E Datei {0} konnte nicht auf fernes Verzeichnis {1} auf Server {2} geladen werden.

Erläuterung: Das Installationsprogramm konnte keine Dateien in das angegebene Verzeichnis auf dem fernen Server kopieren.

Benutzeraktion: Stellen Sie sicher, dass auf dem fernen Server ausreichend Speicherplatz vorhanden ist und dass die vom Installationsprogramm verwendete Benutzer-ID über die entsprechenden Zugriffsrechte und Berechtigungen zum Schreiben von Dateien auf dem fernen Server verfügt.

CIYBA0207E Kein Image für {0} definiert.

Erläuterung: Das Installationsprogramm konnte keine Imagedaten für die Eigenschaftendatei abrufen.

Benutzeraktion: Stellen Sie sicher, dass die Eigenschaftendatei ein Imagefeld mit der Datenkomponente enthält.

CIYBA0208E Image von Komponente {0} konnte nicht auf den fernen Server {1} hochgeladen werden.

Erläuterung: Das Installationsprogramm konnte die Imagedateien nicht in ein Verzeichnis auf dem fernen Server kopieren.

Benutzeraktion: Stellen Sie sicher, dass auf dem fernen Server ausreichend Speicherplatz vorhanden ist und dass die vom Installationsprogramm verwendete Benutzer-ID über die entsprechenden Zugriffsrechte und Berechtigungen zum Schreiben in das Verzeichnis auf dem fernen Server verfügt. Stellen Sie zudem sicher, dass der Name des fernen Verzeichnisses korrekt ist.

CIYBA0209I Hostname : {0}.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0210I OSType={0},OSBit={1},CPUArch={2}.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0211I Ferner Pfad: {0}.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0212I Lokaler Pfad: {0}.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0213E Datei {0} konnte nicht vom fernen Server {1} heruntergeladen werden.

Erläuterung: Das Installationsprogramm konnte die Imagedateien nicht von einem fernen Verzeichnisserver auf den lokalen Server kopieren.

Benutzeraktion: Stellen Sie sicher, dass auf dem lokalen Server ausreichend Speicherplatz vorhanden ist und dass die vom Installationsprogramm verwendete Benutzer-ID über die entsprechenden Zugriffsrechte und Berechtigungen zum Schreiben in das Verzeichnis verfügt. Stellen Sie zudem sicher, dass die lokalen und fernen Verzeichnisnamen korrekt sind.

CIYBA0214E Datei {0} herunterladen.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0215I Befehl: {0}.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0216I Befehlsexitcode : {0}.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0217I Befehlsausgabe: {0}.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0218E Befehl ist mit Rückkehrcode {0} fehlgeschlagen.

Erläuterung: Der Befehl wurde nicht erfolgreich ausgeführt.

Benutzeraktion: Prüfen Sie die Protokolldateien auf weitere Details.

CIYBA0219I Datei {0} hochladen.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0220I Lokales Imageverzeichnis: {0}.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0221I Fernes Imageverzeichnis: {0}.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0222E Fernes Image {0} bereits vorhanden.

Erläuterung: Die Datei ist bereits auf dem Zielserver vorhanden. Im Rahmen des Installationsprozesses werden Medien an Zielserver übertragen. Diese Nachricht gibt an, dass das erforderliche Image bereits übertragen wurde.

Benutzeraktion: Diese Nachricht gibt an, dass Medien aus einem vorherigen Installationsversuch immer noch auf den Zielservern vorhanden sind. Wenn der Benutzer eine neue Installation starten möchte, müssen die Medien gelöscht werden, damit sie erneut hochgeladen werden können.

CIYBA0223E Befehl auf Server {0} kann nicht gestartet werden.

Erläuterung: Das Installationsprogramm konnte den Befehl **`IOC`** vom fernen Server nicht auf dem lokalen Server ausführen.

Benutzeraktion: Prüfen Sie die Verbindung zwischen dem lokalen und dem fernen Server. Stellen Sie sicher, dass die vom Installationsprogramm verwendete Benutzer-ID über entsprechende Zugriffsrechte und Berechtigungen zum Ausführen des Befehls verfügt.

CIYBA0224E Sicherungsdateien vom Ordner {0} auf Server {1} abrufen.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0225E Sicherungsdateien können vom Ordner {0} auf Server {1} nicht abgerufen werden.

Erläuterung: Das Installationsprogramm konnte Dateien von einem fernen Sicherungsordner nicht in einen lokalen Ordner abrufen.

Benutzeraktion: Prüfen Sie die Verbindung zwischen den lokalen und fernen Servern. Stellen Sie sicher, dass die vom Installationsprogramm verwendete Benutzer-ID über entsprechende Zugriffsrechte und Berechtigungen für den Zugriff auf die Ordner verfügt.

CIYBA0226E Auf Server {1} ist kein Sicherungsordner vorhanden: {0}.

Erläuterung: Das Installationsprogramm konnte Dateien von einem fernen Sicherungsordner nicht in einem lokalen Ordner abrufen.

Benutzeraktion: Stellen Sie sicher, dass das ferne Verzeichnis und der Ordner vorhanden sind.

CIYBA0227E Für die ID und das Pfadattribut muss ein Wert angegeben werden.

Erläuterung: Die Installation konnte die Komponenten-ID und das Pfadattribut nicht bestimmen.

Benutzeraktion: Stellen Sie sicher, dass die Komponenten-ID und die Pfadargumente in den Taskargumenten bereitgestellt werden.

CIYBA0228I Exec-Befehl: {0}.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0229E Festplattenspeicher auf Zielverzeichnis{0} nicht ausreichend.

Erläuterung: Das Installationsprogramm hat nicht genügend Speicherplatz im Zielverzeichnis gefunden.

Benutzeraktion: Stellen Sie sicher, dass dem angegebenen Verzeichnis genügend Speicherplatz zugeordnet ist und dass die vom Installationsprogramm verwendete Benutzer-ID darauf zugreifen kann.

CIYBA0230I IOC-Befehlszeilenversion: {0}

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0231I Topologie "{0}" erfolgreich importieren

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0232E Topologiename "{0}" kann im Ordner ../topology nicht gefunden werden

Erläuterung: Das Installationsprogramm konnte die angegebene Topologie im Ordner `../topology` nicht finden.

Benutzeraktion: Stellen Sie sicher, dass die Topologiedatei im Ordner `../topology` vorhanden ist und dass sie ein gültiges XML-Format aufweist.

CIYBA0233I Aktuelle Topologie ist "{0}".

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0234E ANT_HOME wurde nicht oder nicht korrekt festgelegt. Legen Sie ANT_HOME fest.

Erläuterung: Das Installationsprogramm hat einen Fehler in der Umgebungsvariablen `ANT_HOME` festgestellt.

Benutzeraktion: Stellen Sie sicher, dass die Variable `ANT_HOME` auf eine gültige ANT-Version gesetzt ist.

CIYBA0237E Komponenten-ID "{0}" ist ungültig.

Erläuterung: Das Installationsprogramm hat eine falsche Komponenten-ID in der Topologiedatei gefunden.

Benutzeraktion: Stellen Sie sicher, dass die Komponenten-ID vorhanden ist und in der Topologie ordnungsgemäß benannt ist.

CIYBA0238E Aktion "{0}" für Komponenten-ID "{1}" ist ungültig.

Erläuterung: Die angegebene Aktion ist für die aktuelle Komponente in der Topologiedatei falsch.

Benutzeraktion: Prüfen Sie die Topologiedatei und stellen Sie sicher, dass die definierte Aktion für die Komponente geeignet ist.

CIYBA0239E Wenn Sie ausführliche Vorgangsnachrichten wünschen, prüfen Sie {0}.

Erläuterung: Der Befehl wurde nicht erfolgreich ausgeführt.

Benutzeraktion: Prüfen Sie die von {0} angegebene Protokolldatei auf zu ergreifende Maßnahmen.

CIYBA0240I Befehl wurde erfolgreich ausgeführt.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0241E Befehl fehlgeschlagen:

Erläuterung: Der angezeigte Befehl ist fehlgeschlagen.

Benutzeraktion: Die zu ergreifende Maßnahme ist vom fehlgeschlagenen Befehl abhängig. Prüfen Sie den Befehl und die Protokolle, um die Ursache des Fehlers zu bestimmen.

CIYBA0242E Entfernen Sie ".xml" aus Parameter "{0}".

Erläuterung: Der angezeigte Parameter enthält die Dateierweiterung `.xml`.

Benutzeraktion: Parameter für XML-Dateinamen dürfen nicht die Erweiterung `.xml` enthalten. Entfernen Sie `.xml` aus dem Parameter und wiederholen Sie den Befehl.

CIYBA0243E Die Umgebungsvariable IOP_CIPHER_ALG oder IOP_CIPHER_KEYSIZE wurde nicht ordnungsgemäß gesetzt. Setzen Sie die Variablen auf die entsprechenden mit JCE kompatiblen Werte.".

Erläuterung: Das Installationsprogramm konnte keinen korrekten Wert für den in der Verschlüsselung verwendeten Chiffrierwert bestimmen.

Benutzeraktion: Stellen Sie sicher, dass die Umgebungsvariablen `CIPHER_ALG` und `IOP_CIPHER_KEYSIZE` korrekt festgelegt wurden.

CIYBA0244E "{0}" ist kein gültiger Parameter.

Erläuterung: Der angegebene Parameter ist kein gültiger Parameter.

Benutzeraktion: Entfernen oder korrigieren Sie den Parameter und wiederholen Sie den Befehl.

CIYBA0245E Parameter fehlt in "-{0}".

Erläuterung: Der angegebene Parameter ist erforderlich, fehlt jedoch im Befehl.

Benutzeraktion: Wiederholen Sie den Befehl mit dem fehlenden Parameter.

CIYBA0249I Operationsscripts vorbereiten.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0250I Operation abgeschlossen.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0251I Operationssequenz gestartet.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0252I Operationssequenz beendet.

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0253I Images der Komponente [{0}] auf Host [{1}] hochladen

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0254I Komponente [{0}] auf Host [{1}] installieren

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0255I Komponente [{0}] auf Host [{1}] deinstallieren

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0256I Komponente [{0}] auf Host [{1}] starten

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0257I Komponente [{0}] auf Host [{1}] stoppen

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0258I Komponente [{0}] auf Host [{1}] weitergeben

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0259I OK

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0261I {0} Task(s) werden ausgeführt

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0262I Insgesamt werden {0} Task(s) ausgeführt

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0263I Komponente [{0}] auf Host [{1}] sichern

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0264E Protokollkonfigurationsdatei {0} kann nicht geladen werden.

Erläuterung: Die Protokollierungsfunktion kann die Eigenschaftendatei mit den Konfigurationsparametern der Protokollierung nicht finden.

Benutzeraktion: Prüfen Sie, ob das Installationspaket vollständig extrahiert wurde und sich auf einem Dateisystem befindet, auf das die Benutzer-ID, die das Installationsprogramm ausführt, zugreifen kann.

CIYBA0265E Dateihandler für Protokoll kann nicht erstellt werden.

Erläuterung: Die Protokollierungsfunktion konnte eine Datei mithilfe einer Systemdateikennung nicht öffnen.

Benutzeraktion: Lassen Sie die Anzahl der für das System verfügbaren Dateikennungen vom Systemadministrator prüfen. Stellen Sie sicher, dass das Dateisystem, auf dem das Installationspaket extrahiert wurde, nicht beschädigt ist.

CIYBA0266E Das erforderliche RPM-Paket {0} ist auf dem Server {1} nicht installiert.

Erläuterung: Das angegebene RPM-Paket ist auf dem Server nicht installiert.

Benutzeraktion: Installieren Sie das unterstützte RPM-Paket auf dem Server.

CIYBA0267E Auf dem Server {1} steht nicht genügend Festplattenspeicher zur Verfügung.Es ist ein Festplattenspeicher von {0} erforderlich.

Erläuterung: Auf dem Server steht nicht genügend Festplattenspeicher zur Verfügung oder der Server erfüllt nicht die Systemvoraussetzungen für Festplattenspeicher.

Benutzeraktion: Löschen Sie Dateien zur Freigabe von Speicherplatz auf dem Server, um die Mindestanforderungen an Speicherplatz zu erfüllen.

CIYBA0268E Auf dem Server {1} steht nicht genügend Speicherplatz zur Verfügung.Es ist ein Speicherplatz von {0} GB erforderlich.

Erläuterung: Auf dem angegebenen Server steht nicht genügend Arbeitsspeicher zur Verfügung. Der Server erfüllt nicht die Systemvoraussetzungen für die Mindestmenge an Arbeitsspeicher.

Benutzeraktion: Fügen Sie dem Server Arbeitsspeicher hinzu.

CIYBA0269E Das Verzeichnis {0} kann auf dem Server {1} nicht erstellt werden. Das Verzeichnis ist bereits vorhanden.

Erläuterung: Das angegebene Verzeichnis ist auf dem Server bereits vorhanden.

Benutzeraktion: Entfernen Sie das Verzeichnis vom Server.

CIYBA0270E Der TCP-IP-Port {0} ist auf Server {1} bereits im Gebrauch. Dies ist ein erforderlicher Port, der vor der Installation verfügbar sein muss.

Erläuterung: Das Programm oder der Prozess ist be-

reits für die Verwendung eines erforderlichen TCP/IP-Ports auf dem Server konfiguriert.

Benutzeraktion: Konfigurieren Sie den Server neu, sodass der erforderliche Port verfügbar ist. Führen Sie die Installation erneut aus.

CIYBA0271E Server {1} weist nicht den erwarteten vollständig qualifizierten Hostnamen auf. Der erwartete vollständig qualifizierte Hostname lautet {0}.

Erläuterung: Der Server weist nicht den erwarteten vollständig qualifizierten Hostnamen auf.

Benutzeraktion: Geben Sie bei Verwendung der IBM Installation Manager-Installation den vollständig qualifizierten Hostnamen für den Server ein. Geben Sie bei Verwendung der schrittweisen Installation den vollständig qualifizierten Hostnamen im Abschnitt `SERVERS` der Eigenschaftendatei der Topologie ein. Korrigieren Sie den in der Fehlernachricht aufgelisteten Server.

CIYBA0272E Die Netzverbindung von Server {1} zu Server {0} ist unterbrochen.

Erläuterung: Es besteht keine Netzkonnektivität zwischen den zwei angegebenen Servern.

Benutzeraktion: Prüfen Sie die Konnektivität zwischen den Servern. Wenden Sie sich an den Netzadministrator, wenn das Problem bestehen bleibt.

CIYBA0273E Server {0} führt SELinux aus, das nicht unterstützt wird.

Erläuterung: SELinux wird nicht von IBM Intelligent Operations Center unterstützt.

Benutzeraktion: Installieren Sie eine unterstützte Linux-Version.

CIYBA0274E Eine aktive Firewall wurde auf Server {0} erkannt. Alle Firewalls müssen vor der Installation inaktiviert werden.

Erläuterung: Der Server verfügt über eine aktive Firewall.

Benutzeraktion: Inaktivieren Sie die Firewall auf dem Server während des Installationsprozesses.

CIYBA0275E DNS-Eintrag für Server {0} kann nicht gefunden werden. DNS-Suche durch IP oder Hostname ist fehlgeschlagen.

Erläuterung: Der Server ist entweder nicht korrekt im DNS konfiguriert oder der DNS funktioniert nicht ordnungsgemäß. Der DNS-Suchbefehl für den Server anhand der IP-Adresse und des Hostnamens ist fehlgeschlagen.

Benutzeraktion: Wenden Sie sich an den Systemnetzadministrator für den Server und korrigieren Sie den DNS-Eintrag von DNS

CIYBA0276E Eine Systemeinstellung des Servers {1} erfüllt nicht die Installationsvoraussetzungen. Die maximale Anzahl offener Dateien [unlimit] ist kleiner als {0}.

Erläuterung: Die Systemeinstellung für die maximale Anzahl offener Dateien erfüllt nicht die Installationsvoraussetzungen.

Benutzeraktion: Die Einstellung **`ulimit`** muss in den angegebenen Wert geändert werden.

CIYBA0277E Die gefundene Linux-Anforderung erfüllt nicht die Installationsvoraussetzungen. Das erwartete Release ist {0}.

Erläuterung: Die auf dem angegebenen Server installierte Linux-Version wird nicht unterstützt.

Benutzeraktion: Installieren Sie eine unterstützte Linux-Version.

CIYBA0278E Die gefundene Linux-Distribution erfüllt nicht die Installationsvoraussetzungen. Die erwartete Verteilung ist {0}

Erläuterung: Die installierte Linux-Distribution wird nicht unterstützt.

Benutzeraktion: Installieren Sie eine unterstützte Linux-Distribution.

CIYBA0279E Das WebSphere Application Server-Profil {0} wurde nicht gestartet oder das Benutzerkonto bzw. das Kennwort ist auf dem Server {4} ungültig.

Erläuterung: Das WebSphere Application Server-Profil wurde nicht gestartet oder es wurde versucht, es mit ungültigen Berechtigungsnachweisen zu starten.

Benutzeraktion: Starten Sie das WebSphere Application Server-Profil mit einer korrekten Benutzer-ID und einem korrekten Kennwort.

CIYBA0281E Für Server {0} ist IPv6 nicht aktiviert. Aktivieren Sie vor der Installation IPv6 auf dem Server.

Erläuterung: Für den angegebenen Server ist IPv6 nicht konfiguriert.

Benutzeraktion: Aktivieren Sie IPv6 auf dem angegebenen Server.

CIYBA0282E Einige Dateien im Verzeichnis {0} auf dem Media-Server sind beschädigt.

Erläuterung: Alle Installationsdateien verfügen über MD5-Kontrollsummen, die vor der Installation geprüft werden müssen. Die MD5-Kontrollsumme für einige Dateien im angegebenen Verzeichnis ist nicht gültig.

Benutzeraktion: Extrahieren Sie das Installationspaket erneut oder kopieren Sie die Dateien erneut in das Verzeichnis.

CIYBA0283E SSH auf Server {0} ist nicht ordnungsgemäß konfiguriert. Kennwortauthentifizierung mithilfe von SSH ist auf dem Server erforderlich, jedoch nicht konfiguriert.

Erläuterung: Die SSH-Konfiguration auf dem angegebenen Server ist falsch.

Benutzeraktion: Gehen Sie wie folgt vor, um die Datei`/etc/ssh/sshd_config` neu zu konfigurieren:

- Entfernen Sie alle `AllowUsers`-Anweisungen.
- Geben Sie `YES` für `PermitRootLogin` an.
- Geben Sie `YES` für `Password Authentication` an.

Mit diesen Änderungen wird nur `Root`benutzern der Zugriff auf den Server mithilfe von SSH mit Kennwortauthentifizierung erlaubt.

CIYBA0284E Es wurde festgestellt, dass {0} ein symbolischer Softlink ist. Symbolische Links sind nicht zulässig.

Erläuterung: Symbolische oder Softlinks zu Dateien oder Verzeichnissen werden nicht unterstützt.

Benutzeraktion: Entfernen Sie symbolische Links und geben Sie den direkten Pfad oder Dateinamen an.

CIYBA0285E Tivoli Directory Server-Instanz {0} wurde auf Server {1} nicht gestartet.

Erläuterung: Die angegebene Tivoli Directory Server-Instanz muss gestartet werden.

Benutzeraktion: Starten Sie den Tivoli Directory Server.

CIYBA0286E IBM DB2-Instanz {0} wurde auf Server {1} nicht gestartet.

Erläuterung: Die angegebene DB2-Instanz wurde nicht gestartet.

Benutzeraktion: Starten Sie die DB2-Instanz.

CIYBA0287E WebSphere Application Server {1} unter Profil {0} wurde auf Server {2} nicht gestartet.

Erläuterung: Das angegebene WebSphere Application Server-Profil wurde auf dem angegebenen Server nicht gestartet.

Benutzeraktion: Starten Sie das WebSphere Application Server-Profil.

CIYBA0288E "localhost" im Server {0} ist nicht 127.0.0.1 zugeordnet.

Erläuterung: In der Hostdatei für die jeweiligen Server muss `127.0.0.1` dem Eintrag `localhost` zugeordnet sein.

Benutzeraktion: Aktualisieren Sie die Hostdatei auf dem Server, um `127.0.0.1` dem Wert `localhost` zuzuordnen.

CIYBA0289E CPU-Ressourcen von Server {0} reichen nicht aus. Die Anzahl CPU-Ressourcen auf dem Server beträgt {1}

Erläuterung: Die CPU-Ressourcen auf dem Server reichen nicht aus, um die Voraussetzungen zu erfüllen.

Benutzeraktion: Fügen Sie dem angegebenen Server CPU-Ressourcen hinzu.

CIYBA0301E Es wurde auf eine Schaltfläche geklickt, um einen Test auszuführen, jedoch wurden keine passenden Eigenschaften in der Eigenschaftendatei gefunden.

Erläuterung: Die Eigenschaften für den Test wurden in der Eigenschaftendatei nicht gefunden.

Benutzeraktion: Klicken Sie auf **Reset** (Zurücksetzen). Daraufhin liest das Programm die aktuelle Eigenschaftendatei für den Fall, dass Änderungen vorgenommen wurden. Wiederholen Sie den Test.

CIYBA0302E Jeder Test muss über bestimmte Eigenschaften verfügen. "class" ist eine dieser Eigenschaften. Parameter {0}: Klassenname {1}: Methodenname {2}: Folgenummer

Erläuterung: In der Testdefinition fehlt die Klasseneigenschaft.

Benutzeraktion: Suchen Sie nach der Folgenummer in der Eigenschaftendatei. Fügen Sie für den Test eine Klasseneigenschaft hinzu. Dies ist der Klassenname des Tests. Dies ist normalerweise der Klassenname des fernen Ausführungsagenten (der Code, der die Testanforderung zur Ausführung an `IopCatRemoteResponder` weiterleitet.

Beispiel:

0070.classname=com.ibm.iop.cat.fw.remote.IopCatRemoter

CIYBA0303E Jeder Test muss über bestimmte Eigenschaften verfügen. "display label" ist eine dieser Eigenschaften. Parameter: {0}: Klassenname {1}: Methodenname {2}: Folgenummer

Erläuterung: In der Testdefinition fehlt die Anzeigebeschriftung.

Benutzeraktion: Suchen Sie die Folgenummer in der Eigenschaftendatei. Fügen Sie dem Test die Eigenschaft `displaylabel` hinzu. Dies ist der Text, der auf der Schaltfläche angezeigt wird.

CIYBA0304E Es wurde auf eine Schaltfläche geklickt, um einen Test auszuführen, jedoch wurde kein passender Test in der Eigenschaftendatei gefunden.

Erläuterung: Die aktuell geladene Eigenschaftendatei definiert nicht den angeforderten Test.

Benutzeraktion: Klicken Sie auf **Reset** (Zurücksetzen). Die aktuelle Eigenschaftendatei wird neu geladen.

CIYBA0305E Es wurde auf eine Schaltfläche geklickt, um einen Test auszuführen, jedoch wurden keine Konfigurationsdaten für den Test gefunden.

Erläuterung: Für den Test stehen keine Konfigurationsdaten zur Verfügung.

Benutzeraktion: Klicken Sie auf **Reset** (Zurücksetzen). Die aktuelle Eigenschaftendatei wird neu geladen.

CIYBA0306E Der durch die Klasse angegebene Code konnte nicht gefunden werden. Parameter:{0}: Klassenname (nicht gefunden)

Erläuterung: Entweder wurde `classname` in der Eigenschaftendatei nicht ordnungsgemäß angegeben oder der Code wurde nicht gefunden.

Benutzeraktion: Prüfen Sie die gemeinsam genutzten Bibliotheken auf die Anwendung `IopCatRemoteResponder`, um zu ermitteln, ob eine oder mehrere gemeinsam genutzte Bibliotheken fehlen oder nicht angegeben sind.

CIYBA0307E Allgemeine Variablen gelten für alle Tests. Es ist nicht zulässig, den Namen, die Klasse oder Debug mit "Common" festzulegen. Parameter {0}: Klassenname {1}: Methodenname {2}: Eigenschaftsschlüsselzeichenfolge

Erläuterung: `Common` wurde verwendet, um `name`, `class` oder `debug` festzulegen.

Benutzeraktion: Suchen Sie den Schlüssel und entfernen Sie die fehlerhafte Zeile. Beispiel: `common.name` wurde verwendet, um allen Tests denselben Namen zuzuordnen.

CIYBA0308E In Klasse {0}, Methode {1} ist eine Ausnahme aufgetreten. Details {2}

Erläuterung: Es ist eine Ausnahme aufgetreten.

Benutzeraktion: Prüfen Sie die Ausnahmezeichenfolge, um festzustellen, warum der Test fehlgeschlagen ist. Hierbei kann es sich um einen normalen Testfehler handeln. Beispiel: "Connection refused" (Verbindung verweigert) bedeutet normalerweise, dass kein Programm an einem bestimmten Port empfangsbereit war, sodass der Service nicht ausgeführt wird.

CIYBA0309E {0}.{1}() - Test[{2}] - Ausnahme: {3}

Erläuterung: Es ist eine Laufzeitausnahmebedingung im angegebenen Test aufgetreten.

Benutzeraktion: Prüfen Sie die Details der Fehlernachricht.

CIYBA0310E Bei der Ausführung des Tests ist eine unerwartete Ausnahme aufgetreten.

Erläuterung: Es ist eine unerwartete Ausnahme aufgetreten.

Benutzeraktion: Prüfen Sie andere Ausnahmen auf zusätzliche Details.

CIYBA0311I Die vom internen diagnostischen Echotest zurückgegebene Zeichenfolge. Parameter {0}: Eingabeeigenschaften für den Test.

Erläuterung: Zeigt die Eingabeeigenschaften für den Test an.

Benutzeraktion: Dies ist eine normale Nachricht und kein Hinweis auf einen Fehler.

CIYBA0312E Der Web-Test hat den erwarteten HTTP-Antwortcode empfangen (entweder in den 200"s oder durch die Eigenschaft "expectedRcode" angegeben). Parameter: {0}: Klassenname

Erläuterung: Gibt an, dass der Test erfolgreich war.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0313E Der Web-Test hat den erwarteten HTTP-Antwortcode nicht empfangen (entweder in den 200"s oder durch die Eigenschaft "expectedRcode)" angegeben. Parameter: {0}: Klassenname {1}: HTTP-Antwortcode

Erläuterung: Es wurde ein nicht erwarteter HTTP-Antwortcode empfangen.

Benutzeraktion: Prüfen Sie die über die Eigenschaft `hosturl` angegebene URL mit einem Browser oder dem Befehl **wget**.

CIYBA0314E Die Zeichenfolgedarstellung der Testantwort. Parameter: {0}: Antwortcode {1}: Antworttext {2}: zusätzlicher testspezifischer Text

Erläuterung: Diese Nachricht gibt die Testantwort als Zeichenfolge zurück.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYBA0315E Alle Tests müssen über Eigenschaften verfügen. Es wurden keine Eigenschaften an diesen Test übergeben.

Erläuterung: Im Testaufruf haben Eigenschaften gefehlt.

Benutzeraktion: Diese Nachricht sollte nicht erscheinen, da Eigenschaften vom Framework übergeben wurden. Wenden Sie sich an die IBM Softwareunterstützung.

CIYBA0320E Eine erwartete Zeichenfolge wurde in den Texteigenschaften nicht gefunden. Klassenname {0}, Ausgabetext {1}

Erläuterung: Die SSH testet die Anmeldung beim Server, führt die Befehle aus und prüft die Befehlsausgabe auf eine erwartete Zeichenfolge. Es wurde keine erwartete Zeichenfolge in den Eigenschaften für diesen Test angegeben.

Benutzeraktion: Prüfen Sie den Schlüssel `expected` auf den Test. Fügen Sie die Eigenschaft hinzu oder ändern Sie sie, um eine Zeichenfolge anzugeben, die in der Ausgabe für die Befehle erwartet wird, die in der Eigenschaft `commmands` angegeben sind.

CIYBA0322E Erwartete Zeichenfolge in Ausgabe nicht gefunden. Klassenname {0}, Ausgabetext {1}

Erläuterung: Die SSH testet die Anmeldung beim Server, führt die Befehle aus und prüft die Befehlsausgabe auf eine erwartete Zeichenfolge. Die erwartete Zeichenfolge wurde in der Ausgabe nicht gefunden.

Benutzeraktion: Prüfen Sie den Schlüssel `expected` auf den Test und den Ausgabetext. Dies könnte ein Hinweis darauf sein, dass der Test fehlgeschlagen ist. Wenn die Ausgabe die Wortfolge "keyboard interactive not allowed" enthält, könnte das bedeuten, dass die Benutzer-ID oder das Kennwort für die Anmeldung beim fernen Server falsch ist. Prüfen Sie die Eigenschaften `user`, `password` und `hostname` für den Test. Das Kennwort ist ein Alias für ein Kennwort im Schlüsselspeicher.

CIYBA0323E Unerwartete Ausnahme in Klassenname {0}. Ausnahme: {1}

Erläuterung: Es ist eine unerwartete Ausnahme aufgetreten.

Benutzeraktion: Wenn die Ausgabe "keyboard interactive not allowed" enthält, könnte das bedeuten, dass die Benutzer-ID oder das Kennwort für die Anmeldung beim fernen Server falsch ist. Prüfen Sie die Eigenschaften `user`, `password` und `hostname` für den Test. Das Kennwort ist ein Alias für ein Kennwort im Schlüsselspeicher.

CIYBA0340E Der Testausführungsagent (IopCatRemoteResponder) konnte die JSON-Eingabedaten nicht analysieren. Parameter: {0}: Klassenname {1}: Methodenname {2}: POST-Daten

Erläuterung: Die Benutzerschnittstelle und der Testausführungsagent kommunizieren mithilfe von JSON. Dieser Fehler bedeutet, dass der Testausführungsagent (`IopCatRemoteResponder`) die JSON-Eingabedaten nicht analysieren konnte.

Benutzeraktion: Prüfen Sie, ob die POST-Daten das korrekte JSON-Format aufweisen.

CIYBA0341E Bei der Ausführung des Tests ist eine Ausnahme aufgetreten.Parameter: {0}: Klassenname {1}: Methodenname {2}: Ausnahmezeichenfolge

Erläuterung: Bei der Ausführung des Tests ist eine Ausnahme aufgetreten.

Benutzeraktion: Prüfen Sie die Ausnahmezeichenfolge, um festzustellen, warum der Test fehlgeschlagen ist. Hierbei kann es sich um einen normalen Testfehler handeln. Beispiel: "Connection refused" (Verbindung verweigert) bedeutet normalerweise, dass kein Programm am Port empfangsbereit war, sodass der Service nicht ausgeführt wird.

CIYBA0342E Der Testausführungsagent (IopCatRemoteResponder) konnte keine Antwort an die Benutzerschnittstelle zurückgeben. Parameter: {0}: Klassenname {1}: Methodenname {2}: Ausnahmezeichenfolge

Erläuterung: Die Benutzerschnittstelle und der Testausführungsagent kommunizieren mithilfe von JSON. Dieser Fehler bedeutet, dass der Testausführungsagent (`IopCatRemoteResponder`) keine Antwort an die Benutzerschnittstelle zurückgeben konnte.

Benutzeraktion: Prüfen Sie die Ausnahmezeichenfolge, um festzustellen, warum die Antwort nicht gesendet werden konnte. Dieser Fehler kann auftreten, wenn der Test zu lange gedauert hat und die Benutzerschnittstelle nicht länger wartet.

CIYBA0343E Ein erwartetes Schlüsselpräfix fehlt. Parameter: {0}: Klassenname {1}: Methodenname {2}: Eigenschaftsschlüsselzeichenfolge

Erläuterung: Alle Eigenschaften für einen bestimmten Test enthalten als Präfix dieselbe Nummer. Dies ermöglicht eine Gruppierung, da Eigenschaftendateien nicht positionsgebunden sind.

Benutzeraktion: Suchen Sie den Schlüssel in der Eigenschaftendatei und fügen Sie das entsprechende Präfix hinzu. Beispielsweise ist Folgendes nicht korrekt:

```
classname      = com.ibm.iop.cat.fw.remote.IopCatRemoter
0050.rhosturl      = https://${APP_HOSTNAME_1}:9443/IopCatRemoteResponder/IopCatRemoteResponder
0050.remoteclassname= com.ibm.iop.cat.fw.Echo
0050.displaylabel   = Internal Diagnostic (Echo REST remoted)
0050.comment       = Self diagnostic CAT check. Tests link between to CAT modules.
0050.failinfopage   = cct_echo_rest_remoted_test.html
```

Folgendes wäre richtig:

```
0050.classname      = com.ibm.iop.cat.fw.remote.IopCatRemoter
0050.rhosturl      = https://${APP_HOSTNAME_1}:9443/IopCatRemoteResponder/IopCatRemoteResponder
0050.remoteclassname= com.ibm.iop.cat.fw.Echo
0050.displaylabel   = Internal Diagnostic (Echo REST remoted)
0050.comment       = Self diagnostic CAT check. Tests link between to CAT modules.
0050.failinfopage   = cct_echo_rest_remoted_test.html
```

CIYBA0345E Ungültiger Schlüssel - Das Schlüsselpräfix ist nicht numerisch. Parameter: {0}: Klassenname {1}: Methodenname {2}: Folgenummer CCT_RESULTS_INFO = {0}.{1}() - Klasse: {2} Ergebnisse - Antwortcode[{3}] Antworttext[{4}]

Erläuterung: Jeder Test muss über ein numerisches Präfix zur Gruppierung aller Eigenschaften für einen bestimmten Text verfügen. Das angegebene Präfix ist nicht numerisch.

Benutzeraktion: Suchen Sie die Folgenummer in der Eigenschaftendatei. Geben Sie ein numerisches Präfix an und verwenden Sie dasselbe Präfix für die restlichen Eigenschaften für den Test.

CIYBA0347E Es ist eine Ausnahme aufgetreten. Parameter: {0}: Klassenname {1}: Methodenname {2}: Ausnahmezeichenfolge

Erläuterung: Es ist eine Ausnahme aufgetreten.

Benutzeraktion: Prüfen Sie die Ausnahmezeichenfolge, um zu ermitteln, warum der Test fehlgeschlagen ist. Hierbei kann es sich um einen normalen Testfehler handeln. Beispiel: "Connection refused" (Verbindung verweigert) bedeutet normalerweise, dass kein Programm am Port empfangsbereit war, sodass der Service nicht ausgeführt wird.

CIYBA0348E Es wurde auf eine Schaltfläche geklickt, um einen Test auszuführen, jedoch wurden keine passenden Eigenschaften in der Eigenschaftendatei gefunden.

Erläuterung: Es wurden keine Eigenschaften für den Test gefunden. Möglicherweise wurde die Eigenschaftendatei geändert.

Benutzeraktion: Klicken Sie auf **Reset** (Zurücksetzen). Die aktuelle Eigenschaftendatei wird neu geladen.

CIYBA0349E Der durch die Klasse angegebene Code konnte nicht gefunden werden. Parameter:{0}: Klassenname (nicht gefunden)

Erläuterung: Entweder wurde `classname` in der Eigenschaftendatei nicht ordnungsgemäß angegeben oder der Code wurde nicht gefunden.

Benutzeraktion: Prüfen Sie die gemeinsam genutzten Bibliotheken auf die Anwendung `IopCatRemoteResponder`, um zu ermitteln, ob eine oder mehrere gemeinsam genutzte Bibliotheken fehlen.

CIYBA0401E Die Eigenschaftsvorlagendatei "IOPMGMT" wurde nicht angegeben oder sie war nicht korrekt.

Erläuterung: Der Parameter für die Eigenschaftsvorlagendatei "IOPMGMT" fehlt.

Benutzeraktion: Geben Sie den korrekten Namen für die Eigenschaftendatei "IOPMGMT" ein.

CIYBA0402E Die Topologieeigenschaftendatei wurde nicht angegeben oder sie war nicht korrekt.

Erläuterung: Der Parameter für die Topologieeigenschaftendatei fehlt oder ist nicht korrekt.

Benutzeraktion: Geben Sie den korrekten Namen für die Topologieeigenschaftendatei ein.

CIYBA0403E Die Eigenschaftsvorlagendatei "IOPMGMT" wurde nicht angegeben oder sie war nicht korrekt.

Erläuterung: Der Parameter für die Eigenschaftsvorlagendatei "IOPMGMT" fehlt.

Benutzeraktion: Geben Sie den korrekten Dateinamen für die Topologieeigenschaftendatei ein.

CIYBA0404E Die Topologieeigenschaftendatei kann nicht gefunden werden.

Erläuterung: Die Topologieeigenschaftendatei kann nicht gefunden werden.

Benutzeraktion: Stellen Sie sicher, dass sich die Topologieeigenschaftendatei im Verzeichnis *Installationsausgangsverzeichnis*`/topology` auf dem Installationsserver befindet.

CIYBA0405E In der Topologie fehlt ein Kennwort für Eigenschaft:

Erläuterung: In der angegebenen Eigenschaftendatei der Topologie wurde ein Kennwort nicht gefunden.

Benutzeraktion: Ein Kennwort für die Topologiedatei ist erforderlich. Geben Sie ein Kennwort für die Topologie ein.

CIYBA0501E Der erforderliche Parameter für die Cyber Hygiene-Medien der Basisarchitektur fehlt.

Erläuterung: Der erforderliche Parameter für die Cyber Hygiene-Medien von IBM Intelligent Operations Center fehlt.

Benutzeraktion: Prüfen Sie, ob das Cyber Hygiene-Script den korrekten Pfad zur Position der Installationsmedien aufweist.

CIYBA0502E Der erforderliche Parameter für die Topologieeigenschaftendatei fehlt.

Erläuterung: Der Parameter für den Dateinamen für die Topologieeigenschaftendatei fehlt.

Benutzeraktion: Geben Sie den korrekten Dateinamen für die Topologieeigenschaftendatei an.

CIYBA0503E Der erforderliche Parameter für das Cyber Hygiene-Zielverzeichnis der Basisarchitektur fehlt.

Erläuterung: Der erforderliche Parameter für das Cyber Hygiene-Zielverzeichnis fehlt.

Benutzeraktion: Geben Sie das korrekte Zielverzeichnis an.

CIYCC0002E Korrigieren Sie die folgenden Konfigurationsfehler: {0}

Erläuterung: Die Konfigurationsseite zur Bearbeitung von gemeinsamen Sitzungen weist einen Fehler auf. Der Fehler ist durch {0} angegeben.

Benutzeraktion: Korrigieren Sie den Fehler und wiederholen Sie die Anforderung.

CIYCC0005E Das Ereignis kann nicht übergeben werden. Versuchen Sie, das Ereignis erneut zu übergeben. Wenden Sie sich an den Administrator oder den Help-Desk, falls das Problem bestehen bleibt.

Erläuterung: Es ist ein Publisher-Servletfehler aufgetreten, als ein Benutzer versucht hat, ein Ereignis zu aktualisieren, zu eskalieren oder abzubrechen.

Benutzeraktion: Wenden Sie sich an den Administrator oder den Help-Desk zur Behebung des Publisher-Servletfehlers.

CIYCC0006W Der Datensatz wurde von einem anderen Benutzer aktualisiert. Aktualisieren Sie die Seite, um den aktualisierten Datensatz abzurufen.

Erläuterung: Es gibt einen Konflikt zwischen einer Aktualisierungsanforderung des Benutzers und einer anderen Änderung auf dem Server. Dies kann passieren, wenn zwei Benutzer gleichzeitig den Status einer Aktivität ändern. .

Benutzeraktion: Aktualisieren Sie die Seite. Die vom anderen Benutzer vorgenommene Aktualisierung wird angezeigt. Nehmen Sie anschließend die erforderlichen Änderungen vor.

CIYUI0001E Das angegebene JSON-Array enthält Fehler und kann nicht analysiert werden.

Erläuterung: Der Benutzer hat eine JSON-Zeichenfolge in ein Fenster eingegeben, in dem das Script eingegeben werden muss, jedoch weist die Zeichenfolge Syntaxfehler auf und kann nicht analysiert werden.

Benutzeraktion: Korrigieren Sie die JSON-Zeichenfolge.

CIYUI0002E Ereignis nicht gefunden. Die Eigenschaften des Ereignisses können nicht angezeigt werden.

Erläuterung: Die Anforderung zum Anzeigen der Eigenschaften des Ereignisses ist fehlgeschlagen, da die Eigenschaften in der Datenbank nicht gefunden wurden.

Benutzeraktion: Aktualisieren Sie die Seite und wiederholen Sie die Anforderung.

CIYUI0004E Fehler bei der Übergabe der Managerdaten der Positionskarte.

Erläuterung: Beim Festlegen der Managerdaten der Positionskarte ist ein Fehler aufgetreten.

Benutzeraktion: Weitere Details finden Sie in den zusätzlichen Nachrichten.

Zusätzliche Nachrichten auf der Registerkarte "Classifications" (Klassifikationen).

Fehler bei der Datenübergabe
Die neue Klassifikation wurde nicht in die Datenbank eingegeben.

Zusätzliche Nachrichten auf der Registerkarte "Location Maps" (Positionskarten).

Fehler bei der Datenübergabe
Die neue Positionskarte wurde nicht in die Datenbank eingegeben.

Zusätzliche Nachrichten auf der Registerkarte "Areas" (Bereiche).

Die eingegebene Bereichs-ID ist ungültig. Die Bereichs-ID ist bereits auf der Karte vorhanden.
Der Benutzer gibt einen Bereich auf der Karte ein, der bereits vorhanden ist.

Die eingegebene Bereichs-ID ist ungültig.
Die Bereichs-ID ist ungültig. Entweder ist kein

Wert angegeben oder die Bereichs-ID entspricht der übergeordneten Bereichs-ID.

Die eingegebenen Bereichsdaten sind ungültig.
Die Bereichsdaten sind ungültig. Der Kunde muss prüfen, ob in alle erforderlichen Felder für die jeweiligen Bereiche Werte eingegeben wurden.

Die übergeordnete Bereichs-ID darf nicht als Bereich auf der aktuellen Karte angegeben sein.
Die eingegebene übergeordnete Bereichs-ID ist als Bereich auf der Karte vorhanden. Ein Bereich kann nicht über einen übergeordneten Bereich verfügen, der ein Bereich auf der Karte ist. Er muss sich auf einer anderen Karte befinden.

Es bestehen Zirkelbezüge zwischen Bereichen und den zugehörigen übergeordneten Bereichen. Entfernen Sie die Zirkelbezüge.
Entfernen Sie zirkuläre Beziehungen zu übergeordneten Bereichen aus der IBM Intelligent Operations Center-Datenbank.

Fehler bei der Datenübergabe.
Die Registerkarte für neue Bereiche wurde nicht in die Datenbank eingegeben.

CIYUI0003I Data submitted successfully. (Daten erfolgreich gesendet.)

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt. Diese Fehlermeldung gibt an, dass die IBM Intelligent Operations Center-Datenbank, das Positionskartenmanager-Portlet und das Positionskarte-Portlet aktualisiert wurden.

Benutzeraktion: Es ist keine Maßnahme erforderlich.

CIYUI0004I Submitted successfully. (Erfolgreich gesendet.)

Erläuterung: Diese Nachricht ist nur für Informationszwecke bestimmt. Diese Nachricht gibt an, dass die Benutzerschnittstelle des Positionskartenmanager-Portlets gesendet, aber keine Änderungen in der IBM Intelligent Operations Center-Datenbank gespeichert wurden. Wenn keine Änderungen im Positionskartenmanager-Portal eingereicht werden, wird die Aktualisierung abgebrochen.

Benutzeraktion: Klicken Sie auf **Senden**, um die IBM Intelligent Operations Center-Dateien und das Positionskarte-Portlet zu aktualisieren.

Knowledge Base und IBM Support verwenden

In diesem Abschnitt finden Sie Themen zur Verwendung von Knowledge Bases, Fix Central und IBM Support, um Informationen zur Fehlerbehebung zu erhalten.

Wissensdatenbanken durchsuchen

Durch eine Suche in den Wissensdatenbanken von IBM lassen sich häufig Probleme lösen. Mithilfe verfügbarer Ressourcen, Unterstützungstools und Suchmethoden können Sie Ihre Ergebnisse optimieren.

Informationen zu diesem Vorgang

Wenn Sie das Information Center für IBM Intelligent Operations Center durchsuchen, können Sie zwar hilfreiche Informationen finden, in manchen Situationen müssen Sie jedoch auch außerhalb des Information Center nach Antworten auf Ihre Fragen oder nach Problemlösungen suchen.

Vorgehensweise

Verwenden Sie eine oder mehrere der folgenden Methoden, um die Wissensdatenbanken nach erforderlichen Informationen zu durchsuchen:

- Suchen Sie Inhalte mithilfe von IBM Support Assistant Lite (ISA Lite).

  ISA Lite ist ein gebührenfreies Softwaretool, mit dessen Hilfe Ihre Fragen zu IBM Software-Produkten beantwortet und Ihre Probleme mit diesen Produkten gelöst werden können. Weitere Informationen zum Herunterladen und Installieren von ISA Lite erhalten Sie über die Links am Ende des Themas.
- Suchen Sie den benötigten Inhalt über das IBM Unterstützungsportal.

  Das IBM Unterstützungsportal ist eine einheitliche, zentrale Ansicht aller Tools der technischen Unterstützung sowie sämtlicher Informationen für alle Systeme, Softwareprodukte und Services von IBM. Im IBM Unterstützungsportal können Sie zentral auf das elektronische Support-Portfolio von IBM zugreifen. Durch die Anpassung der Seiten haben Sie die Möglichkeit, sich gezielt auf die Informationen und Ressourcen zu konzentrieren, die Sie zur Problemvermeidung und für eine schnellere Problemlösung benötigen. Machen Sie sich mit dem IBM Unterstützungsportal vertraut, indem Sie sich die Demonstrationsvideos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) ansehen, die für dieses Tool verfügbar sind. In diesen Videos erhalten Sie eine Einführung in das IBM Unterstützungsportal und Sie können die Fehlersuche und sonstige Ressourcen erkunden. Außerdem veranschaulichen die Videos, wie Sie die Seite durch das Verschieben, Hinzufügen und Löschen von Portlets anpassen können.
- Suchen Sie Inhalte zu IBM Intelligent Operations Center mithilfe einer der folgenden zusätzlichen technischen Ressourcen:
  - Technische Hinweise und APARs (Problemberichte) zu IBM Intelligent Operations Center
  - IBM Intelligent Operations Center - Seite des Unterstützungsportals
  - IBM Intelligent Operations Center - Seite der Foren und Communitys
  - IBM Smarter Cities Software Solutions Redbooks
- Suchen Sie Inhalte mithilfe der IBM Kopfzeilensuche. Sie können die IBM Kopfzeilensuche verwenden, indem Sie Ihren Suchbegriff in das Suchfeld oben auf einer beliebigen Seite mit der Endung ibm.com eingeben.
- Suchen Sie Inhalte mithilfe einer externen Suchmaschine wie Google, Yahoo oder Bing. Wenn Sie eine externe Suchmaschine verwenden, ist die Wahrscheinlichkeit höher, dass Ihre Ergebnisse Informationen enthalten, die sich außerhalb der Domäne ibm.com befinden. Gelegentlich lassen sich jedoch in Newsgroups, Foren und Blogs außerhalb von ibm.com hilfreiche Informationen zur Problemlösung für IBM Produkte finden.

  Tipp: Wenn Sie Informationen zu einem IBM Produkt suchen, geben Sie in Ihrer Suche „IBM" und den Namen des Produkts ein.

Zugehörige Konzepte:

„Produktinformationen” auf Seite 205
Im Portlet "Produktinformationen" können Sie Details zur Version des IBM Intelligent Operations Center und zur Version der integrierten IBM Smarter Cities Software Solutions anzeigen, die Sie installiert haben. Außerdem können Sie Details zu allen Aktualisierungen anzeigen, die Sie seit der Installation ausgeführt haben.

„IBM Support Assistant Lite installieren und verwenden” auf Seite 320
Das Tool IBM Support Assistant Lite (ISA Lite) sammelt gängige Diagnosedaten, die bei der Analyse allgemeiner Probleme hilfreich sind.

Zugehörige Informationen:

IBM Support Assistant Lite für IBM Intelligent Operations Center 1.5 herunterladen

Fixes von Fix Central abrufen

Mithilfe von Fix Central können Sie die Fixes suchen, die vom IBM Support für eine Vielzahl von Produkten empfohlen werden, u. a. auch für das IBM Intelligent Operations Center. Mit Fix Central können Sie Fixes suchen, auswählen, bestellen und auf Ihr System herunterladen, wobei Sie verschiedene Zustelloptionen auswählen können. Möglicherweise steht ein Produktfix für das IBM Intelligent Operations Center zur Verfügung, mit dem Sie Ihr Problem lösen können.

Vorgehensweise

So suchen und installieren Sie Fixes:

1. Beschaffen Sie sich die Tools, die für den Erhalt des Fixes notwendig sind. Falls dies nicht installiert ist, besorgen Sie sich das Installationsprogramm für die Produktaktualisierung. Sie können das Installationsprogramm von Fix Central herunterladen. Diese Site enthält Download-, Installations- und Konfigurationsanweisungen für das Aktualisierungsprogramm.
2. Wählen Sie IBM Intelligent Operations Center als Produkt aus und aktivieren Sie mindestens ein Kontrollkästchen, das für das Problem relevant ist, das Sie lösen möchten.
3. Bestimmen Sie das erforderliche Fix und wählen Sie es aus.
4. Laden Sie das Fix herunter.
   a. Öffnen Sie das Downloaddokument und folgen Sie dem Link im Abschnitt „Downloadpaket”.
   b. Stellen Sie beim Herunterladen der Datei sicher, dass der Name der Wartungsdatei nicht geändert wird. Diese Änderung kann beabsichtigt sein, oder es kann sich um eine unbeabsichtigte Änderung handeln, die von bestimmten Webbrowsern oder Dienstprogrammen zum Herunterladen verursacht wird.
5. Folgen Sie zum Ausführen des Fix den Anweisungen im Abschnitt „Installationsanweisungen” des Downloaddokuments.
6. Optional: Abonnieren Sie wöchentliche E-Mail-Benachrichtigungen zu Fixes und anderen IBM Supportaktualisierungen.

Zugehörige Tasks:

„Supportaktualisierungen abonnieren” auf Seite 344
Sie können Aktualisierungen abonnieren, damit Sie stets über aktuelle wichtige Informationen zu den von Ihnen verwendeten IBM Produkten verfügen.

Zugehörige Informationen:

Fix Central - Hilfe

IBM Support kontaktieren

Der IBM Support bietet Unterstützung bei Produktfehlern, bei der Beantwortung von häufig gestellten Fragen (FAQs) und bei der Ausführung einer erneuten Erkennung.

Vorbereitende Schritte

Falls Sie mit den Möglichkeiten zur Selbsthilfe wie beispielsweise den technischen Hinweisen keine Antwort auf Ihre Frage oder keine Lösung für Ihr Problem finden konnten, wenden Sie sich an den IBM Support. Bevor Sie den IBM Support kontaktieren, müssen Sie überprüfen, ob Ihr Unternehmen über ein aktives IBM Softwareabonnement und über einen aktiven Unterstützungsvertrag verfügt. Außerdem müssen Sie zum Melden von Problemen an IBM berechtigt sein. Sie finden Informationen zu den Arten des verfügbaren Supports im Abschnitt Support portfolio (Support-Portfolio) des Handbuchs *Software Support Handbook*.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um sich mit einem Problem an den IBM Support zu wenden:

1. Definieren Sie das Problem, stellen Sie Hintergrundinformationen zusammen und bestimmen Sie den Schweregrad des Problems. Weitere Informationen finden Sie im Abschnitt Getting IBM support (IBM Support anfordern) des Handbuchs *Software Support Handbook*.
2. Stellen Sie Diagnoseinformationen zusammen.Weitere Informationen zur Verwendung von IBM Support Assistant Lite zum Erfassen der Protokolldateien von IBM Intelligent Operations Center erhalten Sie über den Link am Ende des Themas.
3. Nutzen Sie eine der folgenden Möglichkeiten, um dem IBM Support das Problem zu melden:
   - IBM Support Assistant Lite verwenden (ISA Lite). Weitere Informationen erhalten Sie über die Links am Ende des Themas.
   - Online über die IBM Intelligent Operations Center - Seite des Unterstützungsportals: Sie können alle Ihre Serviceanforderungen über das Portlet "Service Request" auf der Seite für Serviceanforderungen öffnen, aktualisieren und anzeigen.
   - Telefonisch: Auf der Webseite Directory of worldwide contacts (Verzeichnis weltweiter Kontaktdaten) finden Sie die für Ihre Region gültige Telefonnummer.

Ergebnisse

Falls sich das von Ihnen gemeldete Problem auf einen Softwarefehler oder auf eine fehlende bzw. falsche Dokumentation bezieht, erstellt der IBM Support einen Authorized Program Analysis Report (APAR). Im APAR wird das Problem ausführlich beschrieben. Sofern möglich, stellt Ihnen der IBM Support eine Lösungsstrategie zur Verfügung, die Sie implementieren können, bis das Problem im APAR gelöst wurde und ein Fix bereitgestellt wird. IBM veröffentlicht gelöste Probleme in APARs täglich auf der Website von IBM Support, damit andere Benutzer, bei denen dasselbe Problem auftritt, ebenfalls von dieser Lösung profitieren können.

Nächste Schritte

Bereiten Sie sich auf die Verwendung von IBM Assist On-Site für die Zusammenarbeit mit dem IBM Technical Support-Mitarbeiter vor. Dabei handelt es sich um ein Plug-in für die Unterstützung über Fernzugriff, das Sie auf Ihren Computer herunterladen können. Der IBM Technical Support-Mitarbeiter kann mithilfe von IBM Assist On-Site Ihre Arbeitsoberfläche anzeigen und die Steuerung Ihrer Maus und Ihrer Tastatur übernehmen. Mit diesem Tool kann der benötigte Zeitaufwand für die Problembestimmung, die Erfassung der erforderlichen Daten und die Lösung des Problems verringert werden. Weitere Informationen finden Sie unter IBM Assist On-Site.

Zugehörige Konzepte:

„Produktinformationen” auf Seite 205
Im Portlet "Produktinformationen" können Sie Details zur Version des IBM Intelligent Operations Center und zur Version der integrierten IBM Smarter Cities Software Solutions anzeigen, die Sie installiert haben. Außerdem können Sie Details zu allen Aktualisierungen anzeigen, die Sie seit der Installation ausgeführt haben.

„IBM Support Assistant Lite installieren und verwenden” auf Seite 320
Das Tool IBM Support Assistant Lite (ISA Lite) sammelt gängige Diagnosedaten, die bei der Analyse allgemeiner Probleme hilfreich sind.

Zugehörige Informationen:

IBM Support Assistant Lite für IBM Intelligent Operations Center 1.5 herunterladen

Supportaktualisierungen abonnieren

Sie können Aktualisierungen abonnieren, damit Sie stets über aktuelle wichtige Informationen zu den von Ihnen verwendeten IBM Produkten verfügen.

Informationen zu diesem Vorgang

Wenn Sie Aktualisierungen abonnieren, können Ihnen wichtige technische Informationen und Aktualisierungen für bestimmte IBM Support-Tools und -Ressourcen zugestellt werden. Verwenden Sie eine der folgenden beiden Methoden, um Aktualisierungen zu abonnieren:

RSS-Feeds
Für IBM Intelligent Operations Center steht der folgende RSS-Feed zur Verfügung: *IBM Intelligent Operations Center*.

Sie finden allgemeine Informationen zu RSS einschließlich der ersten Schritte für den Einstieg und einer Liste RSS-fähiger IBM Webseiten auf der Website IBM Software Support RSS feeds.

My Notifications
Mit "My Notifications" können Sie Supportaktualisierungen für jedes beliebige IBM Produkt abonnieren. ("My Notifications" ersetzt "My Support", ein ähnliches Tool, das Sie in der Vergangenheit möglicherweise verwendet haben.) Über "My Notifications" können Sie angeben, dass Sie täglich oder wöchentlich E-Mail-Ankündigungen erhalten möchten. Sie können festlegen, welche Art von Informationen Sie empfangen möchten (beispielsweise Veröffentlichungen, Hinweise und Tipps, Produktflashes (auch als "Alerts" bezeichnet), Downloads und Treiber). "My Notifications" ermöglicht die Anpassung und Kategorisierung der Produkte, über die Sie informiert werden möchten, sowie der Bereitstellungsmethoden, die sich für Sie am besten eignen.

Vorgehensweise

So abonnieren Sie Supportaktualisierungen:

1. Wenn Sie den RSS-Feed für das *IBM Intelligent Operations Center* abonnieren möchten, führen Sie die folgenden Unterschritte aus:
   a. Öffnen Sie den Link IBM Intelligent Operations Center - RSS-Feed.
   b. Wählen Sie im Fenster **Subscribe with Live Bookmark** (Mit dynamischem Lesezeichen abonnieren) einen Ordner aus, in dem Sie das Lesezeichen für den RSS-Feed speichern möchten, und klicken Sie auf **Subscribe** (Abonnieren).

   Sie können weitere Informationen zum Abonnieren von RSS-Feeds über den Link "IBM Software Support RSS feeds" in den Referenzinformationen am Ende dieses Abschnitts aufrufen.
2. Wenn Sie "My Notifications" abonnieren möchten, rufen Sie das IBM Unterstützungsportal auf und klicken Sie im Portlet **Notifications** (Benachrichtigungen) auf **My Notifications** (Meine Benachrichtigungen).
3. Melden Sie sich mit Ihrer IBM ID und mit Ihrem Kennwort an und klicken Sie auf **Submit** (Senden).

4. Geben Sie an, welche Aktualisierungen Sie erhalten möchten, und wie diese bereitgestellt werden sollen.
   a. Klicken Sie auf die Registerkarte **Subscribe** (Abonnieren).
   b. Wählen Sie IBM Intelligent Operations Center aus und klicken Sie auf **Continue** (Weiter).
   c. Wählen Sie Ihre bevorzugte Bereitstellung der Aktualisierungen aus, beispielsweise per E-Mail, online in einem festgelegten Ordner oder als RSS- oder Atom-Feed.
   d. Wählen Sie die Art der Dokumentationsaktualisierungen aus, die Sie empfangen möchten. Zur Auswahl stehen beispielsweise neue Informationen zu Produktdownloads und Kommentare in Diskussionsgruppen.
   e. Klicken Sie auf **Submit** (Senden).

Ergebnisse

Sie erhalten die von Ihnen angeforderten Benachrichtigungen über Aktualisierungen, bis Sie Ihre RSS-Feeds und Ihre Einstellungen von "My Notifications" ändern. Sie können Ihre Einstellungen bei Bedarf jederzeit ändern (wenn Sie beispielsweise ein Produkt nicht mehr verwenden und stattdessen ein anderes Produkt nutzen).

Zugehörige Tasks:

„Fixes von Fix Central abrufen” auf Seite 342
Mithilfe von Fix Central können Sie die Fixes suchen, die vom IBM Support für eine Vielzahl von Produkten empfohlen werden, u. a. auch für das IBM Intelligent Operations Center. Mit Fix Central können Sie Fixes suchen, auswählen, bestellen und auf Ihr System herunterladen, wobei Sie verschiedene Zustelloptionen auswählen können. Möglicherweise steht ein Produktfix für das IBM Intelligent Operations Center zur Verfügung, mit dem Sie Ihr Problem lösen können.

Referenzinformationen

IBM Software Support RSS feeds

Subscribe to My Notifications support content updates

My Notifications für die technische Unterstützung durch IBM

My Notifications für die technische Unterstützung durch IBM - Übersicht

Informationen mit IBM austauschen

Damit ein Problem diagnostiziert oder bestimmt werden kann, müssen Sie dem IBM Support möglicherweise Daten und Informationen aus Ihrem System zur Verfügung stellen. In anderen Fällen kann es hingegen vorkommen, dass Sie vom IBM Support Tools oder Dienstprogramme erhalten, die Sie zur Fehlerbestimmung heranziehen können.

Zugehörige Konzepte:

„Tracing aktivieren und Protokolldateien anzeigen" auf Seite 311
Zur Fehlerbehebung bei Problemen im IBM Intelligent Operations Center müssen Sie möglicherweise Protokolldateien in mehreren Systemen analysieren. In den folgenden Themen erfahren Sie, wie Sie auf die Protokolldateien zugreifen können.

„IBM Support Assistant Lite installieren und verwenden" auf Seite 320
Das Tool IBM Support Assistant Lite (ISA Lite) sammelt gängige Diagnosedaten, die bei der Analyse allgemeiner Probleme hilfreich sind.

Zugehörige Tasks:

„MustGather-Tool bei der Installation ausführen" auf Seite 316
Es werden Protokolldateien erstellt, während IBM Intelligent Operations Center installiert wird. Es ist ein Tool verfügbar, das diese Protokolldateien zur Analyse zusammenstellt.

Zugehörige Informationen:

IBM Support Assistant Lite für IBM Intelligent Operations Center 1.5 herunterladen

Informationen an den IBM Support senden

Sie können den Zeitaufwand für die Problemlösung verringern, indem Sie Trace- und Diagnoseinformationen an den IBM Support senden.

Vorgehensweise

So übergeben Sie Diagnoseinformationen an den IBM Support:

1. Öffnen Sie einen Problem Management Record (PMR) mit dem Serviceanforderungstool.
2. Sammeln Sie die benötigten Diagnosedaten. Durch die Diagnosedaten kann die Lösung Ihres PMR beschleunigt werden. Sie können die Diagnosedaten automatisch oder manuell sammeln:
   - Sammeln Sie die Daten mithilfe von IBM Support Assistant Lite automatisch (ISA Lite). Weitere Informationen erhalten Sie über die Links am Anfang des Themas.
   - Sammeln Sie die Daten manuell.Über die Links am Anfang des Themas erhalten Sie Informationen zu den Protokolldateien des IBM Intelligent Operations Center.
3. Komprimieren Sie die Dateien im ZIP- oder TAR-Format.
4. Übertragen Sie die Dateien an IBM. Nutzen Sie zum Übertragen der Dateien an IBM eines der folgenden Verfahren:
   - Das Serviceanforderungstool
   - Standardverfahren zum Hochladen von Daten: FTP, HTTP
   - Sichere Verfahren zum Hochladen von Daten: FTPS, SFTP, HTTPS
   - E-Mail

   Alle diese Verfahren zum Datenaustausch werden auf der IBM Support-Website erläutert.

Informationen vom IBM Support empfangen

Gelegentlich kann es vorkommen, dass Sie von einem IBM Technical Support-Mitarbeiter gebeten werden, Diagnosetools oder sonstige Dateien herunterzuladen. Sie können diese Dateien über FTP herunterladen.

Vorbereitende Schritte

Vergewissern Sie sich, dass Ihnen der zuständige IBM Technical Support-Mitarbeiter den bevorzugten Server für das Herunterladen der Dateien sowie die genauen Verzeichnis- und Dateinamen für den Zugriff mitgeteilt hat.

Vorgehensweise

So laden Sie Dateien vom IBM Support herunter:

1. Verbinden Sie sich über FTP mit der Website, die Ihnen der zuständige IBM Technical Support-Mitarbeiter genannt hat, und melden Sie sich unter dem Namen `anonymous` an. Verwenden Sie Ihre E-Mail-Adresse als Kennwort.
2. Wechseln Sie in das entsprechende Verzeichnis:
   a. Wechseln Sie in das Verzeichnis `/fromibm`.
      ```
      cd fromibm
      ```
   b. Wechseln Sie in das Verzeichnis, das Ihnen vom zuständigen IBM Technical Support-Mitarbeiter genannt wurde.
      ```
      cd Verzeichnisname
      ```
3. Aktivieren Sie den Binärmodus für Ihre Sitzung.
   ```
   binary
   ```
4. Laden Sie mit dem Befehl **get** die Datei herunter, die der zuständige IBM Technical Support-Mitarbeiter angegeben hat.
   ```
   get Dateiname.Erweiterung
   ```
5. Beenden Sie Ihre FTP-Sitzung.
   ```
   quit
   ```

Bekannte Probleme und Lösungen

Dieser Abschnitt enthält eine Liste häufig auftretender Probleme sowie eine Lösung für die einzelnen Punkte.

Die Key Performance Indicator-Verarbeitung wird nach einer gewissen Zeit abgebrochen

Im IBM Intelligent Operations Center wird die Key Performance Indicator-Verarbeitung (KPI-Verarbeitung) gelegentlich nach einer gewissen Zeit abgebrochen, beispielsweise über Nacht. Sie erhalten Informationen zur Lösung des Problems über den Link am Ende des Themas, der zu den technischen Hinweisen *Die Key Performance Indicator-Verarbeitung wird nach einer gewissen Zeit abgebrochen* für die Fehlerbehebung führt.

Portlets, die bei Änderungen der Sicherheitseinstellungen nicht mit Daten belegt werden

Wenn Portlets nicht erwartungsgemäß mit KPI-, Aktivitäten- oder Ressourcendaten belegt werden, überprüfen Sie die Porteinstellungen. Wenn Sie die Tabelle mit Systemeigenschaften zum Ändern der HTTPS-Einstellungen verwenden und die Porteinstellungen nicht entsprechend ändern, tritt beim Belegen der Portlets mit Daten ein Problem auf.

Verbindungsfehler bei Cognos-Berichten

Wenn Sie einen Verbindungsfehler bei Cognos-Berichten erhalten, müssen Sie die Seite aktualisieren.

Cognos-Berichte werden nicht korrekt angezeigt

Wenn die Cognos-Berichte beim Öffnen der Seite "Aufsichtsperson: Berichte" oder "Betreiber: Berichte" nicht korrekt angezeigt werden, aktualisieren Sie die Seite.

Wenn nach dem Aktualisieren der Seite die Cognos-Berichte weiterhin nicht korrekt angezeigt werden, wurden möglicherweise die Cognos-Anwendungsserver-Cluster gestoppt. Melden Sie sich bei der Web-

Sphere Application Server-Administrationskonsole an und überprüfen Sie den Status der WebSphere Application Server-Cluster. Wenn für den Status eines Clusters ein rotes X angezeigt wird, wählen Sie diesen Cluster aus und drücken Sie **Starten**.

Keine Daten in den Cognos-Berichten

Wenn die Cognos-Berichte nicht korrekt angezeigt werden und die Nachricht `Keine Daten gefunden` angezeigt wird, sind möglicherweise in der Datenbank keine Daten für Ihre Auswahl vorhanden. Definieren Sie Ihre Auswahlkriterien neu. Löschen Sie zum Beispiel die Felder **Anfangsdatum** und **Enddatum** im angepassten Bericht und klicken Sie auf **Aktualisierung**. Kopieren Sie dann die Berichts-URL und fügen Sie sie in das Cognos-Portlet ein.

Bericht wird nicht angezeigt, wenn Sie die Berichts-URL mit der entsprechenden Schaltfläche kopieren

Wenn Sie als Musterbenutzer die Berichts-URL mit der Schaltfläche **Berichts-URL** kopieren und anschließend direkt zur Portletseite für Berichte wechseln, wird der Bericht nicht angezeigt. Um dieses Problem zu beheben, drücken Sie zum Aktualisieren die Taste **F5**. Dann wird der Bericht richtig angezeigt.

Bearbeitete Ressource wird nicht im Portlet "Details" angezeigt

Wenn Sie eine Ressource in Tivoli Service Request Manager bearbeiten und Tivoli Netcool/Impact während dieses Vorgangs nicht verfügbar ist, kann es vorkommen, dass die Ressource nicht im Portlet "Details" angezeigt wird. Wenn Sie beispielsweise auf der Registerkarte **Ereignisse und Vorfälle** mit der rechten Maustaste auf ein Ereignis klicken und anschließend auf **Ressourcen in der Nähe anzeigen** klicken, wird die bearbeitete Ressource möglicherweise nicht angezeigt. Bearbeiten Sie die Ressource zur Lösung des Problems erneut in Tivoli Service Request Manager.

Status der abgemeldeten Benutzer wird im Portlet "Kontakt" nicht richtig angezeigt

Der Status von angemeldeten Benutzern wird im Portlet "Kontakt" angezeigt. Wenn ein angemeldeter Benutzer das Browserfenster schließt oder sich bei WebSphere Portal abmeldet, wird der Status dieses Benutzers weiterhin als angemeldet angezeigt, bis die Sitzung abläuft. Alle Nachrichten, die an diesen Benutzer gesendet werden, nachdem der Benutzer das Browserfenster geschlossen oder sich abgemeldet hat, werden nicht zugestellt. Demzufolge wird dem Benutzer, der versucht, die Nachricht zu senden, eine Fehlernachricht angezeigt. Um sicherzustellen, dass Ihr Status sofort aktualisiert wird, klicken Sie zum Abmelden im Portlet "Kontakt" auf **Datei** > **Abmelden**.

Aktualisierung auf der Seite "Aufsichtsperson: Berichte" mehrmals auswählen

Wenn Sie auf der Seite "Aufsichtsperson: Berichte" an der Benutzerschnittstelle von IBM Intelligent Operations Center den Befehl **Aktualisieren** auswählen, ohne Änderungen vorzunehmen, werden die Felder **Anfangsdatum** und **Enddatum** mit dem aktuellen Datum belegt. Wenn Sie **Aktualisieren** erneut auswählen, ohne Änderungen vorzunehmen, wird die Nachricht `Keine Daten gefunden` angezeigt.

Dieses Verhalten tritt auf, weil die Felder **Anfangsdatum** und **Enddatum** automatisch belegt werden.

Zu lange Überschriften führen zu unbrauchbaren Berichtsdiagrammen

Ereignisüberschriften mit mehr als 20 bis 30 Zeichen können sich darauf auswirken, wie der Kreisdiagrammbericht **Alle Ereignisse, nach Überschrift** angezeigt wird, und dabei das Diagramm unbrauchbar machen. Da die Ereignisüberschriften zur Beschriftung der Kreisdiagrammabschnitte verwendet werden und das Kreisdiagramm so verkleinert wird, dass die Beschriftungen passen, wird die Abbildung des Kreisdiagramms möglicherweise so klein, dass die verschiedenen Abschnitte nicht mehr unterscheidbar sind.

Nicht erwartete Ergebnisse bei der Umrechnung der Browserzeitzone

Unerwartete Ergebnisse bei der Umrechnung der Browserzeitzone werden möglicherweise durch eine falsche Zeitzonencodierung im CAP-Ereignis (Common Alerting Protocol) verursacht. Weitere Informationen erhalten Sie über den Link am Ende des Themas.

Zugehörige Konzepte:

„CAP für KPI-Ereignisse verwenden" auf Seite 103
Der WebSphere Message Broker, der als Teil vom IBM Intelligent Operations Center bereitgestellt wird, akzeptiert CAP-Ereignisnachrichten und verwendet die Dateien in KPI-Berechnungen (Key Performance Indicator).

Zugehörige Informationen:

Technischer Hinweis 'Die Key Performance Indicator-Verarbeitung wird nach einer gewissen Zeit abgebrochen' für die Fehlerbehebung

Verbindungsfehler beim Installieren von IBM Intelligent Operations Center

Maßnahme, wenn während der Installation von IBM Intelligent Operations Center eine SOAPException-Nachricht ausgegeben wird.

Die Verbindung zu einem Server wurde unterbrochen, da eine Nachricht mit etwa folgendem Wortlaut ausgegeben wurde:

```
[SOAPException: faultCode=SOAP-ENV:Client; msg=Read timed out
```

In diesem Fall müssen Sie die Server ausschalten und erneut starten. Starten Sie anschließend das Installationsprogramm neu, oder versuchen Sie erneut, den Installationsbefehl auszuführen.

IPv6-Netzbetrieb startet nicht

Wenn der IPv6-Netzbetrieb auf einem Server nicht startet, sind möglicherweise Änderungen der Datei `/etc/modprobe.conf` erforderlich.

Informationen zu diesem Vorgang

Dieses Problem kann auftreten, wenn ein Upgrade von VMWare auf Version 5 durchgeführt werden soll.

Vorgehensweise

1. Bearbeiten Sie die Datei `/etc/modprobe.conf`.
2. Ändern Sie die folgende Zeile:
   ```
   alias ipv6 off
   ```
   zu
   ```
   # alias ipv6 off
   ```
3. Ändern Sie die folgende Zeile:
   ```
   options ipv6 disable=1
   ```
   zu
   ```
   # options ipv6 disable=1
   ```
4. Speichern Sie die Datei.
5. Starten Sie den Server neu.

Tivoli Service Request Manager startet nicht

Maßnahme, falls Tivoli Service Request Manager vom Plattformsteuerungstool nicht gestartet werden kann und vom Tool Systemprüfung als aktiv angezeigt wird.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um Tivoli Service Request Manager neu zu starten.

Vorgehensweise

1. Stoppen Sie alle Services mithilfe des Plattformsteuerungstool.
2. Beenden Sie den Ereignisserver, und starten Sie ihn anschließend erneut.
3. Starten Sie alle Services mithilfe des Plattformsteuerungstool.

Neue Seite für die Benutzerschnittstelle kann nicht erstellt werden

Beheben Sie ein Problem, das beim Erstellen einer neuen Seite auftritt, wenn Sie mit Microsoft Internet Explorer 9 arbeiten.

Informationen zu diesem Vorgang

Dieses Problem kann auftreten, wenn Sie eine neue Seite über die Seite **Administration** oder über die Benutzerseiten **Stadtübergreifend** erstellen. Die neue Seite wird nicht geladen. Um dieses Problem zu lösen, wechseln Sie vorübergehend den Browser in die **Kompatibilitätsansicht**. Sie müssen sicherstellen, dass **Kompatibilitätsansicht** inaktiviert ist, nachdem Sie eine neue Seite erstellt haben, da IBM Intelligent Operations Center die Kompatibilitätsansicht von Internet Explorer 8 oder Internet Explorer 9 nicht unterstützt.

Vorgehensweise

1. Öffnen Sie Internet Explorer 9.
2. Melden Sie sich bei IBM Intelligent Operations Center als Administrator an.
3. Klicken Sie auf **Administration** > **Portalbenutzerschnittstelle** > **Seiten verwalten**.
4. Klicken Sie aof der oberen Symbolleisten des Browsers auf **Extras**.
5. Wählen Sie aus dem Menü **Kompatibilitätsansicht** aus.
6. Geben Sie `stadtübergreifend` in das Suchfeld ein.
7. Wenn das Suchergebnis zurückgegeben wird, klicken Sie auf **Stadtübergreifend**.
8. Klicken Sie auf die Option für die neue Seite.
9. Wenn die neue Seite geladen wird, kehren Sie zur Browser-Symbolleiste zurück und inaktivieren Sie **Kompatibilitätsansicht**.

Zugehörige Konzepte:

„Unterstützte Browser” auf Seite 15
Die Schnittstelle für IBM Intelligent Operations Center-Lösungen unterstützt eine Reihe von Browsern. Einige Browser können mit Einschränkungen verwendet werden.

Lösungsstrategie für Eingabehilfen für Portlets

Es gibt Lösungsstrategien für Probleme bei Eingabehilfen in Bezug auf einigeIBM Intelligent Operations Center-Portlets:

- In den Portlets "Details" und "Benachrichtigungen" müssen Sie die folgenden Tastatursteuerungen verwenden, um das Kontextmenü aufzurufen:

  Windows
  Drücken Sie die hierfür vorgesehene Menütaste.

Mac Wählen Sie die entsprechende Option aus, die davon abhängt, ob Sie über einen numerischen Tastenblock verfügen:
  - Falls Sie über einen numerischen Tastenblock verfügen, vergewissern Sie sich, dass "Mouse Keys" aktiviert ist, und drücken Sie dann Strg+5.
  - Falls Sie nicht über einen numerischen Tastenblock verfügen, aktivieren Sie "Mouse Keys" und drücken Sie dann Strg+I.

- Klicken Sie zum Öffnen des Fensters **Ereignis hinzufügen** im Portlet "Details" auf die Registerkarte **Ereignisse und Vorfälle** oder drücken Sie die Tabulatortaste. Die Namen der Registerkarten werden vom Sprachausgabeprogramm vorgelesen. Wählen Sie dann die entsprechenden Tastatursteuerungen in der Liste aus.

  Mozilla Firefox
  Strg+Alt+V

  Safari fn+Control+Option+V

  Internet Explorer
  Strg+Alt+V

- Im Fenster **Ereignis hinzufügen** des Portlets "Details" werden die folgenden Werte nicht vom Sprachausgabeprogramm vorgelesen:
  - **Wirksamkeitsdatum**
  - **Wirksamkeitszeit**
  - **Startdatum**
  - **Startzeit**
  - **Ablaufdatum**
  - **Ablaufzeit**

Lösungsstrategie zur Auswahl von Datumsangaben im Portlet "Berichte" im Zusammenhang mit den Eingabehilfen

Im Portlet "Berichte" können Sie mit der Tastatur keine Tage im Kalender auswählen.

Informationen zu diesem Vorgang

Wenn Sie im Portlet "Berichte" einen vordefinierten Bericht konfigurieren möchten, müssen Sie ein Datum oder einen Datumsbereich eingeben. Die Auswahlfunktion für das Kalenderdatum ist jedoch nicht über die Tastatur zugänglich. Der Kalender wird zwar angezeigt, Sie können jedoch mit der Tastatur keine Tage im Kalender auswählen. Die Auswahl von Tagen im Kalender ist nur über die Maus möglich.

Sie können dieses Problem umgehen, indem Sie mithilfe der folgenden Schritte die Tage manuell über die Tastatur eingeben.

Vorgehensweise

1. Wählen Sie im Portlet "Berichte" den vordefinierten Bericht unten auf der Seite aus und klicken Sie auf **Bericht konfigurieren**.
2. Geben Sie im Feld **Anfangsdatum** das Datum ein, für das Informationen angezeigt werden sollen. Wenn Sie einen Datumsbereich eingeben, ist dieses Datum das Anfangsdatum.
3. Geben Sie im Feld **Enddatum** das letzte Datum im Datumsbereich ein, für den Berichtsdaten angezeigt werden sollen.
4. Klicken Sie auf **Bericht anzeigen**.

Neue Ereignisse werden im Details-Portlet nicht angezeigt

Wenn neue Ereignisse im Details-Portlet nicht angezeigt werden, kann dieses Problem in mehreren Schritten behoben werden.

Informationen zu diesem Vorgang

Wenn mit dem ersten Schritt das Problem nicht gelöst wird, fahren Sie mit den nächsten Schritt fort. Fahren Sie so lange mit jedem nächsten Schritt weiter, bis das Problem behoben ist.

Vorgehensweise

1. Überprüfen Sie den Status des IBM Intelligent Operations Center-XML-Testmonitors.
   a. Melden Sie sich beim Ereignisserver als Benutzer `root` an und geben Sie diesen Befehl ein:
      ```
      – tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
      ```
   b. Überprüfen Sie, ob `Connection status OK` (Verbindungsstatus OK) am Ende der Datei angezeigt wird.
   c. Wenn die Meldung `Probe shutting down` (Testmonitor wird gerade beendet) angezeigt wird oder das Datum/die Uhrzeit nicht mit der aktuellen Serverzeit übereinstimmt, führen Sie die folgenden Schritte durch:
      1) Benennen Sie das aktuelle Protokoll mit dem folgenden Befehl um:
         ```
         - mv /opt/IBM/netcool/omnibus/log/ioc_xml.log
         /opt/IBM/netcool/omnibus/log/old_ioc_xml.log
         ```
      2) Starten Sie den Testmonitor mit dem folgenden Befehl neu:
         ```
         /opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc
         ```
      3) Warten Sie ungefähr 1 Minute und geben Sie dann diesen Befehl ein:
         ```
         – tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
         ```
         Suchen Sie nach der Meldung `Connection Status OK` (Verbindungsstatus OK). Wenn der Verbindungsstatus nicht OK ist, prüfen Sie die Datei auf Fehler. Verbindungsprobleme können darauf hinweisen, dass der Objektserver inaktiv ist. Siehe Schritt 2.
2. Wenn der IBM Intelligent Operations Center-XML-Testmonitor weiterhin heruntergefahren wird, führen Sie die folgenden Schritte aus, um den Status der Tivoli Netcool/OMNIbus-Datenbank zu überprüfen. Wenn der IBM Intelligent Operations Center-XML-Testmonitor nicht herunterfährt, fahren Sie mit Schritt 3 fort.
   a. Melden Sie sich beim Ereignisserver als Benutzer `ibmadmin` an und geben Sie diesen Befehl ein:
      ```
      - /opt/IBM/netcool/omnibus/bin/nco_config &
      ```
   b. Wenn Sie zum Importieren aus `omni.dat` aufgefordert werden, wählen Sie **Yes** (Ja) aus und klicken Sie auf **Finish** (Fertigstellen).
   c. Minimieren Sie das Fenster des Prozessagenten und klicken Sie mit der rechten Maustaste auf **NCOMS**.
      Wenn die Option **Connect As** (Verbinden als) verfügbar ist, klicken Sie darauf, stellen Sie eine Verbindung als Benutzer `root` her und verwenden Sie Ihr Topologiekennwort.
      Wenn die Option **Connect As** (Verbinden als) nicht angezeigt wird, schließen Sie `nco_config` und geben Sie als Benutzer `ibmadmin` den folgenden Befehl ein, um den NCOMS-Objektserver zu starten:
      ```
      - /opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
      ```
      Wenn der NCOMS-Objektserver nicht gestartet wird, öffnen Sie `/opt/IBM/netcool/omnibus/var`, suchen Sie die Datei `NCOMS.pid` und benennen Sie sie um. Geben Sie dann folgenden Befehl ein:
      ```
      /opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
      ```

   Anmerkung: Nachdem Sie den NCOMS-Objektserver gestartet haben, müssen Sie den IBM Intelligent Operations Center-XML-Testmonitor neu starten. Siehe Schritt 1.
3. Überprüfen Sie den Status von Tivoli Netcool/Impact.
   a. Melden Sie sich beim Ereignisserver unter "http://*EventsHost*:9080/nci/login_main.jsp" als Benutzer `admin` an.

Wenn Sie sich nicht anmelden können, führen Sie die folgenden Befehle auf dem Ereignisserver aus:

```
su – netcool
/opt/IBM/netcool/bin/ewas.sh start
```

b. Scrollen Sie im Fenster **Service Status** (Servicestatus) nach unten und überprüfen Sie, ob die folgenden Services ausgeführt werden:

- **EventProcessor**
- **IOC_CAP_Event_Reader**
- **IOC_Notification_Reader**

Anmerkung: Ein grünes Häkchen wird neben den ausgeführten Services angezeigt.

c. Klicken Sie im Fenster **Service Status** (Servicestatus) auf das Symbol **View Log** (Protokoll anzeigen) neben **PolicyLogger** und prüfen Sie die Protokolldatei auf Fehler.

Wenn Sie im Protokoll Fehler finden, können Sie Details der Protokolldatei unter `/opt/IBM/netcool/impact/log/` anzeigen. Um weitere Informationen zu erhalten, klicken Sie auf **PolicyLogger**, legen Sie die Option **Highest log level** (Höchste Protokollebene) auf **3** fest und aktivieren Sie die entsprechenden Kontrollkästchen.

4. Überprüfen Sie, ob sich Ereignisse in einer der WebSphere MQ-Warteschlangen befinden.

a. Melden Sie sich mithilfe des VNC-Client beim Ereignisserver an und geben Sie die folgenden Befehle ein, um WebSphere MQ Explorer zu öffnen:

```
xhost +
su - mqm
strmqcfg &
```

Anmerkung: Wenn die Begrüßungsseite geöffnet wird, schließen Sie sie.

b. Erweitern Sie **IBM WebSphere MQ** > **Queue Managers** > **IOC.MC.QM** > **QueuesLocate** (IBM WebSphere MQ > Warteschlangenmanager > IOC.MC.QM > QueuesLocate) und wählen Sie den Ordner **Queues** (Warteschlangen) aus.

c. Aktivieren Sie in der Tabelle **Queues** (Warteschlangen) die Option **Current Queue Depth** (Aktuelle Warteschlangentiefe) für alle Warteschlangen, die mit **IOC_** beginnen. Beispiel: IOC_KPI_IN_INTERNAL_USE_ONLY_DO_NOT_MODIFY.

Eine Warteschlangentiefe, die für einen beliebigen Zeitraum größer als 0 ist, kann auf ein Problem hinweisen.

5. Überprüfen Sie, ob die CAP-Ereignisse die IBM Intelligent Operations Center-Datenbank erreichen.

a. Melden Sie sich mithilfe des VNC-Client beim Datenserver an und geben Sie die folgenden Befehle ein, um DB2 Control Center zu öffnen:

```
xhost +
su - db2inst1
Db2cc &
```

b. Klicken Sie auf **IOCDB** > **tables** (IOCDB > Tabellen). Klicken Sie dann mit der rechten Maustaste auf **Event** (Ereignis) im Schema **IOC_COMMON** und klicken Sie auf **Open** (Öffnen). Es wird eine Liste mit Ereignissen angezeigt, die an das System gesendet wurden.

c. Stellen Sie sicher, dass Ereignisse in der Datenbank vorhanden sind.

Anmerkung: Sie müssen möglicherweise weitere Zeilen abrufen, je nachdem, wie viele Ereignisse im System vorhanden sind.

6. Um die Traceerstellung auf dem Portalserver festzulegen, führen Sie folgende Schritte aus:

a. Melden Sie sich bei der Administrationskonsole unter `http://app-host:9060/ibm/console`, an, wobei `app-host` der vollständig qualifizierte Hostname des Anwendungsservers ist.

b. Klicken Sie auf **Troubleshooting** > **Logs and Trace** (Fehlerbehebung > Protokolle und Trace).

c. Klicken Sie auf **WebSphere_Portal** > **Change log level details** (WebSphere Portal > Details der Protokollstufe ändern).

d. Klicken Sie auf die Registerkarte **Runtime** (Laufzeit), fügen Sie den folgenden Befehl ein und klicken Sie auf **OK**.

```
*=warning: com.ibm.iss.*=all: com.ibm.ioc.*=all
```

e. Geben Sie zum Anzeigen eines Protokolls den folgenden Befehl ein:

```
cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal
tail –f trace.log
```

Weitere Informationen zum Anzeigen von Protokollen erhalten Sie über den Link zum zugehörigen Konzept am Ende des Themas.

Zugehörige Konzepte:

„Tracing aktivieren und Protokolldateien anzeigen" auf Seite 311

Zur Fehlerbehebung bei Problemen im IBM Intelligent Operations Center müssen Sie möglicherweise Protokolldateien in mehreren Systemen analysieren. In den folgenden Themen erfahren Sie, wie Sie auf die Protokolldateien zugreifen können.

Authentifizierungsmechanismus nicht verfügbar

Wenn Sie die Fehlernachricht `HPDIA0119W Authentication mechanism is not available` (Authentifizierungsmechanismus ist nicht verfügbar) erhalten, nachdem Sie sich am WebSphere Portal angemeldet haben, prüfen Sie den Status des Tivoli Directory Server und des Tivoli Directory Server-Proxys für den Anwendungsserver.

Vorgehensweise

1. Melden Sie sich am Verwaltungsserver als `ibmadmin` an und geben Sie die folgenden Befehle ein:

   ```
   su – ibmadmin
   cd /opt/IBM/ISP/mgmt/scripts
   ./iopmgmt.sh  status tds Topologiekennwort
   ```

   Wenn der Server aktiv ist, wird eine Nachricht ähnlich dem folgenden Beispiel angezeigt:

   ```
   Executing query command.....completed.
    IBM Tivoli Directory Server [ on ]
   Command completed successfully.
   ```

2. Wenn der Server nicht aktiv ist, geben Sie `./iopmgmt.sh start tds Topologiekennwort` ein.
3. Wenn der Server nach Ausführung der Schritte 1 und 2 nicht aktiv ist, melden Sie sich am Verwaltungsserver als `ibmadmin` an und geben Sie die folgenden Befehle ein:

   ```
   su – ibmadmin
   cd /opt/IBM/ISP/mgmt/scripts
   ./iopmgmt.sh  status tdspxyapp Topologiekennwort
   ```

   Wenn der Server aktiv ist, wird eine Nachricht ähnlich dem folgenden Beispiel angezeigt:

   ```
   Executing query command.....completed.
   IBM Tivoli Directory Server [ on ]
   Command completed successfully.
   ```

4. Wenn der Server nicht aktiv ist, geben Sie `./iopmgmt.sh start tdspxyappTopologiekennwort` ein.

Server eines anderen Anbieters reagiert nicht

Wenn Sie die Fehlernachricht `Third-party server not responding` (Server eines anderen Anbieters reagiert nicht) erhalten, nachdem Sie sich am WebSphere Portal-Portal angemeldet haben, prüfen Sie den Status des WebSphere Portal.

Vorgehensweise

1. Melden Sie sich am Verwaltungsserver als `ibmadmin` an und geben Sie den folgenden Befehl ein:

   ```
   su – ibmadmin
   cd /opt/IBM/ISP/mgmt/scripts
   ./iopmgmt.sh  status wpe Topologiekennwort
   ```

   Wenn das Portal aktiv ist, wird eine Nachricht ähnlich der folgenden angezeigt:

```
Executing query command.....completed.
IBM WebSphere Portal Extend [ on ]
Command completed successfully.
```

2. Wenn das Portal nicht aktiv ist, geben Sie `./iopmgmt.sh start wpe` *Topologiekennwort* ein.

Im Portlet "Meine Aktivitäten" werden keine Aktivitäten angezeigt

Es gibt mehrere Ursachen, warum im Portlet "Meine Aktivitäten" keine Aktivitäten angezeigt werden. Diese Ursachen werden in den folgenden Abschnitten beschrieben.

Fehlerbehebung mit Beispieldaten

Verwenden Sie zum Erstellen eines Ereignisses die Beispieldaten sowie die Ergebnisse, um die möglichen Ursachen einzuschränken, warum Aktivitäten nicht angezeigt werden.

Vorgehensweise

1. Melden Sie sich bei der IBM Intelligent Operations Center-Verwaltungsschnittstelle als Benutzer `wpsadmin` an.
2. Erstellen Sie das Ereignis "Hurrikan nähert sich":
   a. Klicken Sie im Portlet "Karte" mit der rechten Maustaste in die Karte und klicken Sie dann auf **Ereignis hinzufügen**.
   b. Wählen Sie als **Ereignistyp** den Eintrag **Hurrikan nähert sich** aus. Die anderen Felder werden automatisch gefüllt.
   c. Wählen Sie bei der **Dringlichkeit** den Eintrag **Erwartet** aus.
   d. Behalten Sie die Standardwerte für die anderen Ereignisparameter bei und klicken Sie auf **OK**.

   Die Parameter für das Ereignis "Hurrikan nähert sich" werden einer beispielhaften Standard Operating Procedure in der Auswahlmatrix für Standard Operating Procedure zugeordnet.
3. Überprüfen Sie nach ungefähr 5 Minuten, ob die neue Aktivität für das Ereignis "Hurrikan nähert sich" im Portlet "Meine Aktivitäten" angezeigt wird.

Ergebnisse

- Wenn eine Aktivität für das Ereignis "Hurrikan nähert sich" im Portlet "Meine Aktivitäten" nicht angezeigt wird, kann die Nichtanzeige von Aktivitäten für einen anderen Benutzer daran liegen, dass ein Problem mit Tivoli Service Request Manager vorliegt.
- Wenn eine Aktivität für das Ereignis "Hurrikan nähert sich" im Portlet "Meine Aktivitäten" angezeigt wird, kann die Nichtanzeige von Aktivitäten für einen anderen Benutzer folgende Ursachen haben:
  – Die Benutzerberechtigungen wurden nicht korrekt konfiguriert.
  – Die Standard Operating Procedure wurde nicht korrekt konfiguriert.
  – Die Auswahlmatrix für Standard Operating Procedure wurde nicht korrekt konfiguriert.

Zugehörige Verweise:

„Beispiele für Standard Operating Procedures, Workflows und Ressourcen" auf Seite 146
Beispiele für Standard Operating Procedures, Workflows und Ressourcen werden bereitgestellt, wenn Sie IBM Intelligent Operations Center Version 1.5 installieren.

Status von Tivoli Service Request Manager überprüfen

Wenn beim Erstellen eines Ereignisses mit den Beispieldaten keine Aktivität im Portlet "Meine Aktivitäten" angezeigt wird, folgen Sie der folgenden Prozedur für die Fehlerbehebung von Tivoli Service Request Manager.

Vorbereitende Schritte

Stellen Sie sicher, dass das Verwaltungskennwort von Tivoli Service Request Manager richtig verschlüsselt wurde. Weitere Informationen erhalten Sie über den Link am Ende der Prozedur.

Informationen zu diesem Vorgang

Wählen Sie eine der folgenden Optionen aus.

Vorgehensweise

- Verwenden Sie das Plattformsteuerungstool, um den Status von Tivoli Service Request Manager zu überprüfen:
  1. Melden Sie sich beim Ereignisserver als Benutzer `ibmadmin` mit dem Befehl `putty` an.
  2. Wechseln Sie in das Verzeichnis `opt/IBM/ISP/mgmt/scripts`.
  3. Verwenden Sie das Plattformsteuerungstool, um den Status von Tivoli Service Request Manager abzurufen sowie Tivoli Service Request Manager zu stoppen und zu starten. Weitere Informationen zum Ausführen des Plattformsteuerungstools erhalten Sie über die Links am Ende der Prozedur.
- Sie können Tivoli Service Request Manager auch manuell neu starten. Führen Sie dazu folgende Schritte aus:
  1. Melden Sie sich bei Ereignisserver als Benutzer `ibmadmin` mit dem Befehl `putty` an.
  2. Geben Sie die folgenden Befehle ein, um Tivoli Service Request Manager zu stoppen:

     ```
     cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
     ./stopServer.sh MXServer1 -user waswebadmin -password kennwort
     ./stopNode.sh -user waswebadmin -password kennwort
     ../../ctgDmgr01/bin/stopManager.sh -user waswebadmin -password kennwort
     ```

     Dabei ist *kennwort* das Toplogiekennwort.
  3. Geben Sie die folgenden Befehle ein, um Tivoli Service Request Manager zu starten:

     ```
     cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
     ../../ctgDmgr01/bin/startManager.sh
     ./startNode.sh -user waswebadmin
     ./startServer.sh MXServer1
     exit
     ```

Zugehörige Tasks:

„Status der Services abfragen” auf Seite 212
Das Plattformsteuerungstool ist für die Bestimmung des Status von IBM Intelligent Operations Center-Services verfügbar.

„Services starten” auf Seite 206
Zum Starten von Services, die auf IBM Intelligent Operations Center-Servern ausgeführt werden, ist das Plattformsteuerungstool verfügbar.

„Services stoppen” auf Seite 209
Zum Stoppen von IBM Intelligent Operations Center-Services ist das Plattformsteuerungstool verfügbar.

„Das Verwaltungskennwort von Tivoli Service Request Manager verschlüsseln” auf Seite 64
Verwenden Sie die folgende Prozedur, um das Verwaltungskennwort von Tivoli Service Request Manager in Tivoli Netcool/Impact zu verschlüsseln.

Benutzerberechtigungen überprüfen

Überprüfen Sie, ob ein Benutzer die Berechtigung zum Anzeigen von Aktivitäten in Verbindung mit der Standard Operating Procedure hat.

Vorgehensweise

1. Um das Standard Operating Procedures-Portlet zu öffnen, klicken Sie in der WebSphere Portal-Verwaltungsschnittstelle auf **Intelligent Operations** > **Customization Tools** > **Standard Operating Procedures** (Intelligent Operations > Anpassungstools > Standard Operating Procedures).
2. Um die Anwendung "Auswahlmatrix für Standard Operating Procedures" zu öffnen, klicken Sie auf **Auswahlmatrix für Standard Operating Procedures**.

3. Suchen Sie in der Spalte **Name der SOP** den Namen der Standard Operating Procedure, für die Sie die Benutzerberechtigungen überprüfen möchten.
4. Klicken Sie neben dem Feld **Name der SOP** auf das Symbol **Detail Menu** (Detailmenü) und klicken Sie anschließend auf **Go To Standard Operating Procedure** (Zur Standard Operating Procedure wechseln).
5. Klicken Sie neben dem Feld **Owner Group** (Eignergruppe) auf das Symbol **Detail Menu** (Detailmenü) und klicken Sie anschließend auf **Go To Person Groups Procedure** (Zur Person Groups Procedure wechseln).
6. Überprüfen Sie, ob der Benutzer Mitglied der Personengruppe ist.

Nächste Schritte

Wenn der Benutzer kein Mitglied der Personengruppe ist, führen Sie eine der folgenden Aktionen durch:

- Verleihen Sie keine Benutzerberechtigung zum Anzeigen von Aktivitäten in Verbindung mit der Standard Operating Procedure.
- Fügen Sie den Benutzer zur Personengruppe hinzu, sodass der Benutzer alle Aktivitäten anzeigen kann, die der Personengruppe zugeordnet sind.
- Fügen Sie den Benutzer einer anderen Personengruppe zu, die mit der Standard Operating Procedure verbunden ist.

Weitere Informationen zum Konfigurieren von Benutzern erhalten Sie über den Link am Ende dieser Task.

Zugehörige Tasks:

„Neue Benutzer in Tivoli Service Request Manager konfigurieren” auf Seite 133
Wenn Sie einen Benutzer in IBM Intelligent Operations Center hinzufügen, ordnen Sie Berechtigungen und Personengruppen für den Benutzer in Tivoli Service Request Manager zu.

Verbindung eines Workflows mit einer Standard Operating Procedure überprüfen

Erstellen Sie ein Ereignis, dessen Parameter den Auswahlkriterien entsprechen, die Sie in der Auswahlmatrix für Standard Operating Procedure definiert haben. Überprüfen Sie, ob die zugehörigen Workflowaktivitäten im Portlet "Meine Aktivitäten" angezeigt werden.

Informationen zu diesem Vorgang

Weitere Informationen zu jedem der folgenden Schritte erhalten Sie über die Links am Ende der Prozedur.

Vorgehensweise

1. Erstellen Sie einen Workflow.
2. Erstellen Sie eine Standard Operating Procedure und verbinden Sie sie mit dem Workflow, den Sie im vorherigen Schritt erstellt haben.
3. Erstellen Sie einen Eintrag für die Standard Operating Procedure in der Auswahlmatrix für Standard Operating Procedure.
4. Erstellen Sie im Portlet "Karte" ein Ereignis, das den Parametern entspricht, die Sie in der Auswahlmatrix für Standard Operating Procedure definiert haben.
5. Überprüfen Sie, ob die zugehörigen Workflowaktivitäten im Portlet "Meine Aktivitäten" angezeigt werden.

Nächste Schritte

Wenn im Portlet "Meine Aktivitäten" keine Aktivitäten angezeigt werden, überprüfen Sie, ob Sie den Workflow, die Standard Operating Procedure, die Auswahlmatrix für Standard Operating Procedure und das Ereignis korrekt konfiguriert haben. Wenn die Konfiguration korrekt ist, überprüfen Sie die Tivoli Netcool/OMNIbus-Richtlinienprotokolldatei und die Tivoli Service Request Manager-Protokolldateien.

Zugehörige Konzepte:

„Karte” auf Seite 294
Mit dem Portlet "Karte" können Sie die in einer Karte enthaltenen Ereignisse und Ressourcen anzeigen.

„Meine Aktivitäten” auf Seite 300
Im Portlet "Meine Aktivitäten" wird eine dynamische Liste mit Aktivitäten angezeigt, deren Eigner die Gruppe ist, zu der der an der Schnittstelle angemeldete Benutzer gehört.

Zugehörige Tasks:

„Workflows erstellen” auf Seite 136
In Tivoli Service Request Manager können Sie Workflows erstellen, die Sie als automatische Tasks in Ihre Standard Operating Procedure-Aktivitäten einschließen können.

„Standard Operating Procedures erstellen” auf Seite 136
Erstellen Sie eine Standard Operating Procedure und ordnen Sie sie einer Eignergruppe zu. Benutzer werden Eignergruppen über ihre Zugehörigkeit zu einer Personengruppe zugeordnet.

„Parameter in der Auswahlmatrix für Standard Operating Procedure definieren” auf Seite 139
Definieren Sie in der Auswahlmatrix für Standard Operating Procedure die Ereignisparameter, die bestimmen, ob eine Standard Operating Procedure für ein bestimmtes Ereignis ausgewählt wird.

Protokolldateien überprüfen

Überprüfen Sie die Tivoli Netcool/OMNIbus-Richtlinienprotokolldatei und die Tivoli Service Request Manager-Protokolldatei.

Vorgehensweise

- Überprüfen Sie die Tivoli Netcool/OMNIbus-Richtlinienprotokolldatei:
  1. Aktivieren Sie die Tivoli Netcool/OMNIbus-Richtlinienprotokolldatei. Weitere Informationen zum Aktivieren und Verwenden der Protokolldatei erhalten Sie über den Link am Ende der Prozedur.
  2. Suchen Sie in der Tivoli Netcool/OMNIbus-Richtlinienprotokolldatei nach `CallMaximoEnterpriseServices`, um nach einem Ereignis zu suchen. Die Tivoli Netcool/OMNIbus-Richtlinienprotokolldatei parst Ereignisse nach Parameter, z. B. `Category` oder `Severity`, und listet jedes Ereignis mit der zugehörigen Arbeitsauftrags-ID auf. Sie können alle Ereignisse mit der Auswahlmatrix für Standard Operating Procedure abgleichen. Wenn ein Ereignis in der Tivoli Netcool/OMNIbus-Richtlinienprotokolldatei nicht aufgelistet wird, liegt dies daran, dass keine Standard Operating Procedure den Ereignisparametern entspricht.
  3. Suchen Sie nach `server error 500`. Dieser Fehlercode gibt an, dass ein Tivoli Service Request Manager-Serverfehler vorliegt. Wenn diese Fehlermeldung angezeigt wird, überprüfen Sie die Tivoli Service Request Manager-Protokolldatei. Siehe Link am Ende der Prozedur.
- Überprüfen Sie die Tivoli Service Request Manager-Protokolldatei. Weitere Informationen zum Aktivieren und Verwenden der Protokolldatei erhalten Sie über den Link am Ende der Prozedur.

Zugehörige Tasks:

„Tivoli Netcool/Impact-Protokolldateien aktivieren und anzeigen” auf Seite 315

„Tracing und Anzeigen von Protokolldateien für Tivoli Service Request Manager aktivieren” auf Seite 312

Nicht in Status- oder Key Performance Indicator - Drilldown-Portlets angezeigte KPI-Daten

Wenn KPI-Daten in Status oder in Key Performance Indicator - Drilldown-Portlets nicht angezeigt werden, führen Sie die folgenden Schritte der Prozedur aus, um das Problem zu beheben.

Vorgehensweise

1. Um den Status von IBM WebSphere Business Monitor zu überprüfen, melden Sie sich bei der WebSphere Application Server-Administrationskonsole an. Weitere Informationen zum Zugreifen auf Administrationskonsolen erhalten Sie über den Link am Ende des Themas.
2. Wenn IBM WebSphere Business Monitor gestoppt wurde, starten Sie es neu. Wenn IBM WebSphere Business Monitor nicht gestoppt wurde, stoppen Sie es und starten Sie es neu. Wenn das Problem nicht behoben wurde, führen Sie Schritt 3 durch.
3. Prüfen Sie die IBM WebSphere Business Monitor-Protokolle, um Probleme mit IBM WebSphere Business Monitor zu finden und zu beheben. Weitere Informationen zum Prüfen von Protokollen erhalten Sie über den Link am Ende des Themas.
4. Wenn alle IBM WebSphere Business Monitor-Probleme behoben sind, melden Sie sich bei der WebSphere Application Server-Administrationskonsole an, um IBM WebSphere Business Monitor neu zu starten.

Zugehörige Konzepte:

„Protokolldateien des Anwendungsservers” auf Seite 311
Mit den folgenden Prozeduren können Sie für einige der Systeme auf dem Anwendungsserver das Tracing aktivieren und Protokolle anzeigen.

„Administrationskonsolen” auf Seite 213
Mit dem Portlet "Administrationskonsolen" können Sie die Services verwalten, die von der Lösung bereitgestellt werden.

Nicht in Status oder in Key Performance Indicator - Drilldown-Portlets aktualisierte Ereignisse

Wenn KPI-Ereignisdaten in Status oder in Key Performance Indicator - Drilldown-Portlets nicht aktualisiert werden, führen Sie die folgenden Schritte der Prozedur aus, bis Sie das Problem behoben haben.

Vorgehensweise

1. Um zu bestätigen, dass KPI-Ereignisaktualisierungen an IBM Intelligent Operations Center gesendet werden, navigieren Sie zum Link *Neue Ereignisse werden im Details-Portlet nicht angezeigt* am Ende des Themas und führen Sie die Schritte aus.
2. Bestätigen Sie, dass Ereignisse an IBM WebSphere Business Monitor gesendet werden.
   a. Melden Sie sich bei der WebSphere Application Server-Administrationskonsole an. Weitere Informationen zum Zugreifen auf Administrationskonsolen erhalten Sie über den Link am Ende des Themas.
   b. Klicken Sie auf **Troubleshooting** > **Monitor Models** > **Failed Event Sequences** (Fehlerbehebung > Monitormodelle > Fehlgeschlagene Ereignissequenzen). Löschen Sie alle KPI-Ereignisse, die auf dieser Seite angezeigt werden.
   c. Starten Sie IBM WebSphere Business Monitor erneut.
   d. Klicken Sie auf **Applications** > **Monitor Services** > **Recorded Events Management** > **Enable/Disable Events Record** (Anwendungen > Überwachungsservices > Aufgezeichnete Ereignisverwaltung > Ereignisaufzeichnung aktivieren/inaktivieren) und aktivieren Sie die Ereignisaufzeichnung.
   e. Klicken Sie auf **Applications** > **Monitor Services** > **Recorded Events Management** > **Events Management** (Anwendungen > Überwachungsservices > Aufgezeichnete Ereignisverwaltung > Ereignisverwaltung). Überprüfen Sie auf dieser Seite, dass mindestens zwei Ereignisse für jedes KPI-Ereignis erstellt wurden, das an IBM Intelligent Operations Center gesendet wird.
3. Bestätigen Sie, dass KPI-Ereignisaktualisierungen an das Portlet "Key Performance Indicators (KPIs)" gesendet werden. Weitere Informationen zum Portlet "Key Performance Indicators (KPIs)" erhalten Sie über den Link am Ende des Themas. Wenn im Portlet "Key Performance Indicators (KPIs)" aktualisierte KPI-Werte angezeigt werden, wurden die Werte in IBM WebSphere Business Monitor aktualisiert.

Zugehörige Konzepte:

„Administrationskonsolen” auf Seite 213
Mit dem Portlet "Administrationskonsolen" können Sie die Services verwalten, die von der Lösung bereitgestellt werden.

„Key Performance Indicators (KPIs)” auf Seite 178
Mit dem Portlet "Key Performance Indicators (KPIs)" können Sie KPIs (Key Performance Indicator) und ihre hierarchische Anzeige in IBM Intelligent Operations Center anpassen.

Zugehörige Tasks:

„Neue Ereignisse werden im Details-Portlet nicht angezeigt” auf Seite 351
Wenn neue Ereignisse im Details-Portlet nicht angezeigt werden, kann dieses Problem in mehreren Schritten behoben werden.

Kapitel 10. Referenz

Diese Themen enthalten zusätzliche Referenzinformationen, die hilfreich sind.

In IBM Intelligent Operations Center eingeschlossene Produkte und Komponenten

Die IBM Intelligent Operations Center-Lösung installiert eine Reihe von Softwareprodukten und -komponenten.

Die Softwareprodukte und -komponenten und die Server, auf denen sie installiert sind, sind in Tabelle 100 angegeben.

Tabelle 100. Mit IBM Intelligent Operations Center installierte Produkte

Produkt	Anwendungsserver	Datenserver	Ereignisserver	Verwaltungsserver
IBM WebSphere Business Monitor 7.5	installiert	nicht installiert	nicht installiert	nicht installiert
IBM Cognos Business Intelligence 10.1.1	installiert	nicht installiert	nicht installiert	nicht installiert
DB2 Enterprise Server Edition mit DB2 Spatial Extender 9.7.0.5	nicht installiert	installiert	nicht installiert	installiert
Semantic Model Services	nicht installiert	nicht installiert	nicht installiert	installiert
IBM ILOG CPLEX Optimization Studio 12.4	installiert	nicht installiert	nicht installiert	nicht installiert
Jazz Foundation Server (für Semantic Model Services) 3.0.1	nicht installiert	nicht installiert	nicht installiert	installiert
Lotus Domino 8.5.3.1	nicht installiert	nicht installiert	installiert	nicht installiert
Lotus Sametime Standard 8.5.2 + IFR1	nicht installiert	nicht installiert	installiert	nicht installiert
Tivoli Access Manager for e-Business 6.1.1.4	nicht installiert	nicht installiert	nicht installiert	installiert
Tivoli Composite Application Manager 7.1	nicht installiert	nicht installiert	nicht installiert	installiert
Tivoli Directory Integrator 7.1.0.5	nicht installiert	nicht installiert	nicht installiert	installiert
Tivoli Directory Server 6.3.0.8	nicht installiert	installiert	nicht installiert	nicht installiert
Tivoli Identity Manager 5.1	nicht installiert	nicht installiert	nicht installiert	installiert
Tivoli Monitoring 6.2.2.1	nicht installiert	nicht installiert	nicht installiert	installiert

Tabelle 100. Mit IBM Intelligent Operations Center installierte Produkte (Forts.)

Produkt	Anwendungsserver	Datenserver	Ereignisserver	Verwaltungsserver
Tivoli Netcool/ Impact 5.1.1.1 + IF003	nicht installiert	nicht installiert	installiert	nicht installiert
Tivoli Netcool/ OMNIbus 7.3.1.2 und XML-Testmonitor	nicht installiert	nicht installiert	installiert	nicht installiert
Tivoli Service Request Manager 7.2.1.2	nicht installiert	nicht installiert	installiert	nicht installiert
WebSphere Application Server 1.1.0.0 Feature-Pack für Web 2.0 und Mobile	installiert	nicht installiert	nicht installiert	nicht installiert
WebSphere Application Server Network Deployment 7.0.0.21	installiert	nicht installiert	nicht installiert	installiert
WebSphere Application Server 6.1.0.29 for Tivoli Service Request Manager	nicht installiert	nicht installiert	installiert	nicht installiert
WebSphere Message Broker 8.0	nicht installiert	nicht installiert	installiert	nicht installiert
WebSphere MQ 7.0.1.7	nicht installiert	nicht installiert	installiert	nicht installiert
WebSphere Operational Decision Management 7.5.1 (Rules Engine)	installiert	nicht installiert	nicht installiert	nicht installiert
WebSphere Portal Enable 7.0.0.2	installiert	nicht installiert	nicht installiert	nicht installiert

Unter dem Account `root` ausgeführte Prozesse

Nachdem Cyber Hygiene ausgeführt wird, müssen einige Prozesse unter dem Account `root` ausgeführt werden.

Prozesse, die unter dem Account `root` ausgeführt werden, können anfällig sein, wenn ein Benutzer oder Prozess `root`-Berechtigungen über eine Berechtigungseskalation erhält. Dies ist in der Regel ein Problem für Services, die von einem Benutzer veranlasste Anforderungen verarbeiten. Vom Benutzer veranlasste Anforderungen können böswillig konfigurierte Eingaben enthalten, die den Server beeinträchtigen können. Services, die Benutzeranforderungen verarbeiten, sind Systeme, die Benutzerschnittstellen oder zugängliche Anwendungsprogrammierschnittstellen (APIs) bereitstellen.

Für Linux-Daemons besteht normalerweise dieses Risiko nicht, da sie nur starten, stoppen oder auf klar strukturierte Ereignisse reagieren. Diese Daemons müssen häufig als `root`-Account ausgeführt werden, sodass sie andere Prozesse steuern oder auf kritische Systemereignisse reagieren können. So lange ein von Benutzern zugänglicher Server nicht als `root` ausgeführt wird, stellen Daemons, die unter dem `root`-Account ausgeführt werden, keine besondere Gefährdung dar.

Mit Ausnahme von Tivoli Netcool/OMNIbus sind alle Produktserver in IBM Intelligent Operations Center unter IDs konfiguriert, die keine Systemberechtigungen haben. Tivoli Netcool/OMNIbus stellt Überwachungs- und Verwaltungsservices auf allen IBM Intelligent Operations Center-Hosts und -Servern bereit.

In Tabelle 101 werden die Prozesse aufgelistet, die weiterhin als `root`-Account ausgeführt werden, nachdem Cyber Hygiene ausgeführt wurde.

Tabelle 101. IBM Intelligent Operations Center-Umgebungsprozesse, die als `root` ausgeführt werden

Server	Produkt	Prozessname	Erläuterung
Datenserver und Verwaltungsserver	DB2	`db2wdog`	Dieser Daemonprozess empfängt Systemereignisse und gibt diese an mehrere untergeordnete Prozesse weiter. Der `db2wdog`-Prozess verwaltet die `db2sync`-Prozesse und erfordert eine Stammebenenverwaltung.
Datenserver und Verwaltungsserver	DB2	`db2chkpwd`	Dieser Daemon authentifiziert die Benutzer-ID und das Kennwort des Benutzers oder der Anwendung, der bzw. die eine Verbindung zur Datenbank herstellen. Der `db2chkpwd`-Prozess muss die Kennwortdatei `/etc/shadow` lesen.
Datenserver und Verwaltungsserver	DB2	`/opt/IBM/DB2/bin/db2fmcd`	Dieser Daemon fungiert als Fehlerüberwachungskoordinator. Er muss als `root` ausgeführt werden, um alle DB2-Instanzen zu überwachen.
Datenserver und Verwaltungsserver	DB2	`/usr/sbin/rcst/bin/rmcd` und `/usr/sbin/rcst/bin/IBM.ConfigRMd`	Diese Befehle verwalten die Hochverfügbarkeitslösung für DB2. Sie müssen auf alle Datenbanken auf den Servern, die für eine Hochverfügbarkeit konfiguriert wurden, zugreifen können.
Ereignisserver	IBM Tivoli Monitoring-Agenten für Lotus Domino	`kgbagent`, `kgbclient`, `kslagent`	Diese Überwachungsagenten müssen als `root` ausgeführt werden, um die Lotus Domino-Serveraktivität nachverfolgen zu können.
Anwendungsserver, Ereignisserver und Verwaltungsserver	IBM HTTP Server	`httpd -d`, `http -f`	Linux benötigt einen `root`-Zugriff, um Ports kleiner als 1024 zu überwachen. Die Standard-HTTP-Ports sind 80 bis 443. IBM Intelligent Operations Center verwendet Port 82. Die Prozesse `httpd -d` und `http -f` müssen als `root` ausgeführt werden. Für jede alternative Konfiguration ist die Installation als Teil eines umfassenden Netzwerks und einer Sicherheitsrichtlinie und -Konfiguration zuständig.
Datenserver	IBM Tivoli Monitoring-Agenten	`klzagent`, `kcawd`	Dies sind Überwachungs- und Verwaltungsagentprozesse. Diese Prozesse überwachen Betriebssystem- und Anwendungsprozesse sowie Ressourcen.
Anwendungsserver	IBM Tivoli Monitoring-Agenten	`klzagent`, `kcawd`, `khtagent`, `kynagent`	Dies sind Überwachungs- und Verwaltungsagentprozesse. Diese Prozesse überwachen Betriebssystem- und Anwendungsprozesse sowie Ressourcen.
Ereignisserver	IBM Tivoli Monitoring-Agenten	`klzagent`, `kcawd`, `khtagent`, `kynagent`, `kmcrca`, `kgbagent`, `kgbstart.sh`, `kgbclient`, `kslagent`, `kmqagent`, `/opt/IBM/ITM/JRE/lx8266/bin/java`	Dies sind Überwachungs- und Verwaltungsagentprozesse. Diese Prozesse überwachen Betriebssystem- und Anwendungsprozesse sowie Ressourcen.
Verwaltungsserver	IBM Tivoli Monitoring-Agenten	`cms`, `kdsmain`, `KfwServices`, `klzagent`, `kcawd`, `kynagent`, `/opt/IBM/ITM/li6263/iw/java/jre/bin/java`, `/opt/IBM/ITM/li6263/iw/java/bin/java`	Dies sind Überwachungs- und Verwaltungsagentprozesse. Diese Prozesse überwachen Betriebssystem- und Anwendungsprozesse sowie Ressourcen.
Ereignisserver	Tivoli Netcool/OMNIbus	`/usr/ibm/common/acsi/jre/bin/java`, `/opt/IBM/netcool/omnibus/platform/linux2x26/bin/nco_pad`	Der Prozess `nco_pad` ist der Prozessagent-Daemon, der alle Prozessagenten überwacht. Der Daemon benötigt Zugriff auf die Systemressourcen. Der Prozessagent-Daemon stellt keine Benutzerschnittstelle dar. Er verwaltet nur andere Prozesse.

Cyber Hygiene-Ausnahmen

Sobald Cyber Hygiene ausgeführt wird, bleiben bekannte Ausnahmen zur bevorzugten Sicherheitskonfiguration bestehen.

Eine ideale Konfiguration hat keine Ausnahmen bei den Best-Practice-Einstellungen. Die meisten Systeme müssen jedoch Ausnahmen haben. Diese Ausnahmen stellen kein besonders hohes Risiko dar, können aber problematisch sein, wenn sie nicht verstanden werden. Einige Programme müssen beispielsweise mit dem Bitset **suid** ausgeführt werden.

Sicherheitsadministratoren müssen die Ausnahmen kennen, sodass sie überprüfen können, ob ihr System beeinträchtigt ist. Beim Scannen kennen Systemadministratoren den Unterschied zwischen beabsichtigten Ausnahmen und Malware.

Tabelle 102. Cyber Hygiene-Ausnahmen zur bevorzugten Sicherheitskonfiguration

Schwachstelle	Server	Instanz	Erläuterung
GEN000360: GID set to value in the system range for Linux (0-499) [GID auf Wert im Systembereich für Linux (0-499) festgelegt].	Datenserver	`dasadm1`	Die Gruppen-ID (GID) `dasadm1` wird auf 102 festgelegt. Dies ist die Verwaltungsgruppe für die DB2-Laufzeitinstanz-IDs. Diese Gruppe wird automatisch erstellt, wenn DB2 installiert wird.

Dateiberechtigungen mit notwendiger Systemadministratorbewertung

Cyber Hygiene nimmt keine Änderungen für Risiken in Dateiberechtigungen und Eigentumsrechten vor. Diese müssen von Systemadminstratoren bewertet und korrigiert werden, da automatische Änderungen dazu führen können, dass einige Systemfunktionen nicht mehr funktionieren.

Die Cyber Hygiene-Scripts protokollieren Informationen zu potenziell betroffenen Ressourcen. Systemadministratoren können diese Ergebnisse überprüfen und entsprechende Systemänderungen vornehmen.

Die Ergebnisdateien befinden sich im Verzeichnis `/var/BA15/CH/results` auf jedem IBM Intelligent Operations Center-Server. Der Dateiname lautet `scanrem-combined-log-`*`date-time`*`.log`. Mit der Zeitmarke wird angegeben, ob Cyber Hygiene ausgeführt wurde.

In Tabelle 103 werden Schwachstellen sowie empfohlene Aktionen aufgelistet, die überprüft werden müssen.

Tabelle 103. Vom Systemadministrator zu bewertende Schwachstellen

STIGID	Beschreibung	Schweregrad	Empfehlung
GEN001220	Dateien, Anwendungen und Verzeichnisse in den Systemverzeichnissen müssen einem Systemaccount oder einem Anwendungsaccount gehören.	II	Überprüfen Sie das Eigentumsrecht der Ressource und führen Sie ggf. eine manuelle Änderung oder Dokumentation durch.
GEN001240	Dateien, Anwendungen und Verzeichnisse in den Systemverzeichnissen müssen einer Systemgruppe oder einer Anwendungsgruppe gehören.	II	Überprüfen Sie die Gruppenzugehörigkeit der Ressource und führen Sie ggf. eine manuelle Änderung oder Dokumentation durch.
GEN001500	Das Ausgangsverzeichnis, das für einen Benutzer in der Datei `/etc/password` aufgelistet wird, muss einem Benutzer gehören.	II	Überprüfen Sie das Eigentumsrecht des Ausgangsverzeichnisses und ändern Sie das Eigentumsrecht manuell oder dokumentieren Sie, warum es nicht geändert werden kann.

Tabelle 103. Vom Systemadministrator zu bewertende Schwachstellen (Forts.)

STIGID	Beschreibung	Schweregrad	Empfehlung
GEN001520	Das Ausgangsverzeichnis, das für einen Benutzer in der Datei `/etc/password` aufgelistet wird, muss einer Primärgruppe eines Benutzers gehören.	II	Überprüfen Sie die Gruppenzugehörigkeit des Ausgangsverzeichnisses und ändern Sie die Gruppenzugehörigkeit manuell oder dokumentieren Sie, warum sie nicht geändert werden kann.
GEN001560	Dateien im Ausgangsverzeichnis, die keine Startdateien sind, dürfen eine maximale Berechtigung von 750 haben.	III	Ändern Sie Berechtigungen, wenn Ausnahmen noch nicht dokumentiert wurden.
GEN002520	Öffentliche Verzeichnisse müssen dem `root`-Account oder einer Anwendungsbenutzer-ID gehören.	II	Überprüfen Sie das Eigentumsrecht und weisen Sie es ggf. zu.
GEN002540	Öffentliche Verzeichnisse müssen `root`, `sys`, `bin` oder einer Anwendungsgruppe gehören.	II	Überprüfen Sie die Gruppenzugehörigkeit und weisen Sie sie ggf. zu.

Zertifizierungen der Produkt- und Komponentensicherheit

Einige Produkte und Komponenten der IBM Intelligent Operations Center-Lösung besitzen Sicherheitszertifizierungen.

Tabelle 104. Mit IBM Intelligent Operations Center installierte Produkte mit Sicherheitszertifizierungen

	Allgemeine Kriterien		FIPS 140-2		
Produkt	Release	Stufe	Release	Zertifizierung?	IPV6
IBM WebSphere Business Monitor	Keine	Keine	7.5	Ja	Ja
IBM Cognos Business Intelligence	10.1.1	Keine	Keine	Keine	Ja
DB2 Enterprise Server Edition mit DB2 Spatial Extender	9.7	EAL4+ALC_FLR.1	9.1 FP2	Ja	Ja
IBM HTTP Server	7.0.0.19		7.0	Ja	Ja
Lotus Domino	Keine	Keine	8.0.1	Ja	Ja
Lotus Sametime Standard	Keine	Keine	8.5	Ja	Ja
Tivoli Access Manager for e-Business	6.0 FP3	EAL3+ALC_FLR.1	6.0	Ja	Ja
Tivoli Composite Application Manager	Keine	Keine	Keine	Keine	Ja
Tivoli Directory Integrator	Keine	Keine	7.0	Ja	Ja
Tivoli Directory Server	6.2	EAL4+ALC_FLR.1	6.1	Ja	Ja
Tivoli Identity Manager	5.0	EAL3+ALC_FLR.1	Keine	Keine	Ja
Tivoli Monitoring	Keine	Keine	6.2.0.1	Ja	Ja
Tivoli Netcool/Impact	Keine	Keine	5.1	Ja	Ja
Tivoli Netcool/OMNIbus und XML-Testmonitor	7.1	EAL2	Alle	Ja	Ja
Tivoli Service Request Manager	Keine	Keine	Alle	Ja	Ja
WebSphere Application Server Network Deployment	6.1.0.2	EAL4+ALC_FLR.1	Alle	Ja	Ja
WebSphere Application Server for Tivoli Service Request Manager	6.1.0.2	EAL4+ALC_FLR.1	Alle	Ja	Ja
WebSphere Message Broker	6.0.0.3	EAL4+ALC_FLR.2 (de)	6.1	Ja	Ja
WebSphere MQ	6.0.1.1.	EAL4+ALC_FLR.2	Alle	Ja	Ja
WebSphere Operational Decision Management (Rules Engine)	Keine	Keine	Keine	Keine	Ja

Tabelle 104. Mit IBM Intelligent Operations Center installierte Produkte mit Sicherheitszertifizierungen (Forts.)

	Allgemeine Kriterien		FIPS 140-2		
Produkt	**Release**	**Stufe**	**Release**	**Zertifizierung?**	**IPV6**
WebSphere Portal Enable	5.0	EAL2	Alle	Ja	Ja

Produkte mit FIP 104-2 sind zertifiziert, weil in der Regel IBM Crypto for C- and Java-Module verwendet werden. Die Zertifikatsnummern für diese Produkte finden Sie in Tabelle 105.

Tabelle 105. FIPS 140-2-Zertifikate

Modul	**Zertifikatsnummer**
IBM Crypto for C (V8.0.0)	1433
IBM CryptoLite for Java (V4.2)	910
IBM CryptoLite for C (V4.5)	899
IBM Java JCE 140-2, Verschlüsselungsmodul	497
IBM Java JSSE FIPS 140-2, Verschlüsselungsmodul	409
IBM SSL Lite for Java	406

Zugehörige Informationen:

Allgemeine Kriterien: http://www.commoncriteriaportal.org/

Sicherheitsbewertungen von IBM Produkten

PDF-Bibliothek

Dieser Abschnitt enthält Links zum Inhalt des Information Center im PDF-Format.

Der Inhalt des Information Center steht als folgende PDF-Version zur Verfügung, damit Sie die Informationen schnell ausdrucken können:

- IBM Intelligent Operations Center Information Center

Glossar

Dieses Glossar enthält Begriffe und Definitionen für IBM Intelligent Operations Center.

Die folgenden Querverweise werden in diesem Glossar verwendet:

- Siehe verweist von einem Begriff auf ein bevorzugtes Synonym oder von einem Akronym bzw. einer Abkürzung auf den definierten ausgeschriebenen Begriff.
- Siehe auch verweist auf einen zugehörigen Terminus oder auf ein Antonym.

Wenn Sie Glossare zu anderen IBM Produkten anzeigen möchten, rufen Sie die Webseite www.ibm.com/software/globalization/terminology auf. (Öffnet sich in einem neuen Fenster.)

A

Abstract Syntax Notation One (ASN.1)
Internationaler Standard für die Definition der Syntax von Informationsdaten. Er definiert einige einfache Datentypen und legt eine Notation für die Bezeichnung dieser Typen sowie für die Angabe ihrer Werte fest. Die ASN.1-Notationen können angewandt werden, wenn die abstrakte Syntax von Informationen definiert werden muss, ohne deren Verschlüsselung für die Übertragung in irgendeiner Form zu beschränken.

ACL Siehe Zugriffssteuerungsliste.

Administratorberechtigung
Die Berechtigung, die einem Administrator erteilt wird und ihm Erstellungs-, Konfigurations- und Löschzugriff für Portalressourcen oder -benutzer gewährt. Diese Berechtigung wird im Rahmen der Mitgliedschaft in einer Benutzerrollengruppe erteilt.

Aggregations-KPI
Ein KPI-Wert, der auf der Grundlage einer Metrik unter Verwendung einer Aggregationsfunktion berechnet wird.

Alert Eine Nachricht, die ein Ereignis oder eine Key-Performance-Indicator-Statusänderung signalisiert.

Alert-Trigger
Eine vordefinierte Änderung des Key Performance Indicator-Werts (KPI-Werts), die bewirkt, dass eine Alertbenachrichtigung an das Portlet "Coordinator - Alerts" gesendet wird.

Allgemeines Widget
Ein Widget, das von IBM bereitgestellt wird und keinem bestimmten Produkt zugeordnet ist. Siehe auch Widget.

Anpassung

1. Die Änderung einer Portalseite oder eines Portlets durch einen Benutzer. WebSphere Portal ermöglicht es dem Benutzer, eine Portalseite anzupassen, indem das Seitenlayout geändert und angegeben wird, welche Portlets für die einzelnen Einheiten angezeigt werden sollen. Siehe auch Personalisierung.
2. Der Prozess des Beschreibens wahlfreier Änderungen in Standardwerte eines Softwareprogramms, das bereits auf dem System installiert und konfiguriert ist, sodass es verwendet werden kann. Siehe auch Konfiguration.

APAR -Siehe Authorized Program Analysis Report.

ASN.1 -Siehe Abstract Syntax Notation One.

Asynchron
Betrifft Ereignisse, die zeitlich nicht synchronisiert sind oder nicht in regelmäßigen oder vorhersehbaren Zeitintervallen auftreten.

Attribut
Ein Merkmal oder eine Eigenschaft einer Entität, die diese beschreibt; z. B. ist die Telefonnummer eines Mitarbeiters eines der Attribute des Mitarbeiters.

Auftrag (WO)
Eine Eintragung, die Informationen über zu erledigende Arbeit enthält.

Ausdrucks-KPI
Ein KPI, dessen Wert auf Basis der Werte anderer KPIs errechnet wird.

Auswahlmatrix für Standard Operating Procedures
Eine Matrix, die eindeutige Ereignisparameterfolgen enthält, die bestimmen, ob eine Standard Operating Procedure für ein bestimmtes Ereignis eingeleitet wird.

Authentifizierung
Ein Sicherheitsservice, der nachweist, dass ein Benutzer eines Computersystems wirklich die Person ist, die er vorgibt zu sein. Einheitliche Verfahren zur Implementierung dieses Service sind Kennwörter und digitale Signaturen.

Authorized Program Analysis Report (APAR)
Eine Anforderung zur Korrektur eines Mangels bei einem unterstützten Release eines von IBM bereitgestellten Programms.

Autorisierung
Das Verfahren bei dem einem Benutzer, System oder Prozess entweder vollständiger oder eingeschränkter Zugriff auf ein Objekt, eine Ressource oder eine Funktion gewährt wird.

Autorisierungsberechtigung
Zugriff auf ein Portal, eine Ressource oder auf Daten im Rahmen einer Gruppenmitgliedschaft.

B

Basiskarte
Eine Karte, die Hintergrundreferenzinformationen wie Landschaftsformen, Straßen, Landmarken und politische Grenzen darstellt, worauf weitere thematische Informationen aufbauen. Eine Basiskarte, die oft einen geodätischen Steuerungsnetzplan als Teil ihrer Struktur enthält, wird als Standortverweis eingesetzt.

Benutzeradministrator
Eine Person, die neue Benutzer hinzufügt und Sicherheit bietet, indem sie Benutzerzugehörigkeiten mit entsprechender Berechtigung in rollenbasierten Berechtigungsgruppen erteilt.

Benutzerberechtigung
Die Berechtigung, die einem Benutzer gewährt wurde, um Zugriff auf Portalressourcen zu erhalten und mit ihnen arbeiten zu können. Diese Berechtigung wird im Rahmen der Mitgliedschaft in einer Benutzerrollengruppe erteilt.

Benutzerprofil
Die Beschreibung eines Benutzers, die Informationen wie Benutzer-ID, Benutzername, Kennwort, Zugriffsberechtigung und andere Attribute enthält, die beim Anmelden angefordert werden.

Benutzerrollengruppe
Eine Gruppe, die Mitgliedschaft zuweist, sodass neue Benutzer die entsprechende Zugriffsstufe für eine Lösung erhalten. Jeder neue Benutzer wird der entsprechenden Rollengruppe als Mitglied hinzugefügt. Jeder Rollengruppe sind jeweils unterschiedliche Berechtigungsstufen zugeordnet.

Betriebsansicht
Eine Webseite mit Portlets, durch deren Zusammenarbeit die Bereitstellung umfassender Informa-

tionen und die Interaktion auf Betriebsebene für die Überwachung aktueller Ereignisse und die Planung künftiger Ereignisse vereinfacht werden.

Breitengrad
Der Winkelabstand eines Ortes vom Äquator, nördlich oder südlich davon gelegen. Er wird für gewöhnlich in Grad und Minuten ausgedrückt.

C

Cache Speicher, der einen schnelleren Zugriff auf Anweisungen oder Daten oder auf beides ermöglicht. Daten, die sich im Cache befinden, sind gewöhnlich Kopien von Daten, die sich woanders auf langsameren, weniger speicherintensiven Speichermedien wie einer Festplatte oder einem anderen Netzknoten befinden.

CAP Siehe Common Alerting Protocol.

Cloudanwendung
Eine Anwendung, die erweitert wird, sodass über das Internet darauf zugegriffen werden kann. Cloudanwendungen verwenden große Rechenzentren und leistungsstarke Server, die Webanwendungen und Web-Services hosten.

Common Alerting Protocol (CAP)
Ein einfaches, aber allgemeines Format für den Austausch von allgemein gültigen Notfallgefahrenalerts und von öffentlichen Warnungen über alle Netzarten hinweg.

CSV-Datei
Eine Textdatei, die durch Kommas getrennte Werte enthält. Eine CSV-Datei wird häufig zum Austauschen von Dateien zwischen Datenbanksystemen und Anwendungen genutzt, die unterschiedliche Formate verwenden.

D

Dashboard
1. Eine Webseite, die einen oder auch mehrere Widgets umfassen kann, mit deren Hilfe Geschäftsdaten grafisch dargestellt werden können.
2. Eine Schnittstelle, die Daten aus verschiedenen Quellen integriert und eine vereinheitlichte Anzeige der relevanten und signifikanten Informationen bereitstellt.

Datenkategoriegruppe
Eine Gruppe, deren Mitglieder auf bestimmte Datenkategorien zugreifen können, beispielsweise auf medizinische Daten und Daten des Gesundheitswesens oder auf Umweltdaten. Durch die Zuweisung der Mitgliedschaft in einer Datenkategoriegruppe erhält ein Benutzer die entsprechende Zugriffsebene für Daten. Jeder Benutzer wird der entsprechenden Gruppe bzw. den entsprechenden Gruppen als Mitglied hinzugefügt.

Datenzugriffsberechtigung
Zugriff auf Daten in einer bestimmten Kategorie, beispielsweise auf medizinische Daten und Daten des Gesundheitswesens oder auf Umweltdaten. Dieser Zugriff ist einer Datenkategoriegruppe zugeordnet.

Direkthilfe
Erläuternder Text, der angezeigt werden kann, indem der Cursor über ein Element der grafischen Benutzerschnittstelle geführt wird (beispielsweise über ein Symbol, ein Feld oder eine Textfolge). Die Direkthilfe kann hilfreiche Texte und Links enthalten.

Domäne
Ein einzelner Bereich einer übergeordneten Organisation, der sich in der Regel aus der Organisationsstruktur und dem Fachwissen der beteiligten Personen ergibt. Eine Stadtverwaltung ist beispielsweise in Bereiche aufgeteilt, die sich mit dem Transport-, dem Wasserwesen und öffentlicher Sicherheit befassen.

E

EAR Siehe Unternehmensarchiv.

EJB Siehe Enterprise JavaBeans.

Enterprise JavaBeans (EJB)
Eine von Sun Microsystems definierte Komponentenarchitektur für die Entwicklung und Implementierung objektorientierter, verteilter Unternehmensanwendungen (Java EE).

Ereignis
Eine wichtige Begebenheit, die an einem bestimmten Ort und zu einer bestimmten Zeit stattfindet. Siehe auch Störung.

Ereigniskorrelation
Der Prozess der Analyse von Ereignisdaten zur Identifizierung von Mustern, allgemeinen Fehlerursachen und der eigentlichen Fehlerursache. Bei der Ereigniskorrelation werden die eingehenden Ereignisse auf vordefinierte Statuszustände hin geprüft, und zwar anhand vordefinierter Regeln und im Kontext vordefinierter Beziehungen.

Extensible Markup Language (XML)
Eine auf der Standard Generalized Markup Language (SGML) basierende Standardmetasprache zum Definieren von Auszeichnungssprachen.

F

Filterformular
Ein Formular, mit dem der Benutzer den Inhalt auswählen kann, der auf der Karte und in der Liste angezeigt werden soll.

Formdatei
Ein digitales Dateiformat für Software von geografischen Informationssystemen.

G

GDDM
Siehe Graphical Date Display Manager.

Geografisches Informationssystem (GIS)
Ein Komplex aus Objekten, Daten und Anwendungen, mit dem räumliche Informationen zu geografischen Objekten erstellt und analysiert werden.

Geografisch-räumlich
Die geografischen Merkmale der Erde betreffend.

GIS Siehe Geografisches Informationssystem .

Graphical Date Display Manager (GDDM)
Ein IBM Computergrafiksystem, das Texte und Grafiken zur Bildschirmanzeige oder zum Ausdrucken definiert und anzeigt.

Gruppe
Eine Gruppe von Benutzern, die die Zugriffsberechtigungen für geschützte Ressourcen gemeinsam verwenden können.

H

Heapspeicher
In der Java-Programmierung ein Speicherblock, der von der Java Virtual Machine (JVM) zur Laufzeit für das Speichern von Java-Objekten verwendet wird. Der Java-Heapspeicher wird von einem Garbage-Collector verwaltet, der automatisch die Zuordnung von Java-Objekten aufhebt, die nicht mehr in Gebrauch sind.

I

Integration
Die Softwareentwicklungsaktivität, bei der separate Softwarekomponenten kombiniert werden und zusammen eine ausführbare Einzellösung bilden.

ISO-Modell
Eine Gruppe von Regeln für die Datenübertragung, die von der "International Organization for Standardization" (ISO) genehmigt wurde. Die ISO-Protokolle ermöglichen die Verbindung und den Kommunikationsaustausch von Systemen, die von unterschiedlichen Herstellern stammen. Sie sind die Basis der Standards für die Kommunikation offener Systeme (OSI).

J

J2EE Siehe Java Platform, Enterprise Edition.

JAR Siehe Java-Archiv.

Java-Archiv (JAR)
Ein Format für komprimierte Dateien, mit dem alle Ressourcen, die zur Installation und Ausführung eines Java-Programms erforderlich sind, in einer einzigen Datei gespeichert werden können. Siehe auch Unternehmensarchiv.

Java EE
Siehe Java Platform, Enterprise Edition.

Java Naming and Directory Interface (JNDI)
Eine Erweiterung der Java-Plattform, die eine Standardschnittstelle zu heterogenen Benennungs- und Verzeichnisservices bereitstellt.

Java Platform, Enterprise Edition (J2EE, Java EE)
Eine Umgebung zur Entwicklung und Implementierung von Unternehmensanwendungen (Enterprise Applications), die von Oracle definiert wurde. Die Java EE-Plattform besteht aus einem Servicepaket, Anwendungsprogrammierschnittstellen (APIs) und Protokollen, die die Funktionalität für die Entwicklung von webbasierten Anwendungen mit mehreren Ebenen bereitstellen. (Sun)

JavaScript Object Notation (JSON)
Ein einfaches Datenaustauschformat, das auf der Objekt-Literal-Notation von JavaScript basiert. JSON ist programmiersprachenneutral, verwendet allerdings Konventionen aus Sprachen, wie C, C++, C#, Java, JavaScript, Perl und Python.

Java Virtual Machine (JVM)
Die Softwareimplementierung eines Prozessors, die kompilierten Java-Code (Applets und Anwendungen) ausführt.

JNDI Siehe Java Naming and Directory Interface.

JSON Siehe JavaScript Object Notation.

JVM Siehe Java Virtual Machine.

K

Keyhole Markup Language (KML)
Ein XML-Grammatik- und -Dateiformat zur Modellierung und Speicherung geografischer Objekte wie Punkte, Linien, Grafiken und Polygone.

Key Performance Indicator (KPI)
Eine quantifizierbare Kennzahl, die zur Protokollierung eines der strategisch wichtigen Erfolgsfaktoren entwickelt wurde, die für einen Geschäftsprozess gelten.

KML Siehe Keyhole Markup Language.

Konfiguration

1. Die Art, mit der die Hardware und die Software eines Systems, Subsystems oder Netzes aufgebaut und miteinander verbunden sind.
2. Der Prozess des Beschreibens von installierten Einheiten, Zusatzeinrichtungen und Lizenzprogrammen einem System gegenüber, sodass diese verwendet werden können. Siehe auch Anpassung.

KPI Siehe Key Performance Indicator.

KPI-Modell
Der Teil des Überwachungsmodells, der den KPI-Kontext enthält, der seinerseits die wesentlichen Leistungsindikatoren (KPI = Key Performance Indicator) sowie die zugehörigen Auslöser und Ereignisse enthält.

KPI-Richtlinie
Eine Richtlinie, die bestimmt, ob ein eingehendes Ereignis als KPI-Ereignisaktualisierung gilt und anschließend zur Verarbeitung gesendet wird, um (je nach Parameter) eine KPI-Aktualisierung oder einen Alert zu generieren.

L

Längengrad
Der Winkelabstand eines Ortes östlich oder westlich des Nullmeridians von Greenwich, England, gewöhnlich in Grad und Minuten ausgedrückt.

Layer Ein Overlay, das auf die Karte gelegt werden kann, um weitere Geodaten bereitzustellen.

LDAP Siehe Lightweight Directory Access Protocol.

LDAP Directory Interchange Format (LDIF)
Ein Dateiformat, mit dem sowohl die Verzeichnisinformationen als auch Änderungen beschrieben werden, die in einem Verzeichnis aufgeführt werden müssen, damit die Verzeichnisinformationen zwischen Verzeichnisservern, die PDAP verwenden, ausgetauscht werden können.

LDIF Siehe LDAP Directory Interchange Format.

Lightweight Directory Access Protocol (LDAP)
Ein offenes Protokoll, das TCP/IP für den Zugriff auf die Verzeichnisse, die ein X.500-Modell unterstützen, verwendet und die Ressourcenanforderungen des komplexeren X.500-DAP-Modells nicht erfüllt. LDAP kann z. B. zum Suchen von Personen, Organisationen und weiteren Ressourcen in einem Internet- oder Intranetverzeichnis verwendet werden.

Lineare Referenz
Eine Referenzmarkierung zur Positionsbestimmung an einer Straße. Sie befindet sich für gewöhnlich am Randstreifen und gibt die jeweilige Streckenposition an. Ein Beispiel für eine Markierung ist ein Kilometerpfosten.

Logische Zoneneinteilung
Eine logische Zusammenfassung von Assets oder Ereignissen innerhalb eines geografischen Bereichs.

LOS Siehe Verkehrsqualität (Level of Service, LOS).

Lösung
Eine Kombination von Produkten, die sich mit einem bestimmten Kundenproblem befasst oder auf ein spezielles Projekt zugeschnitten ist.

M

Motiv Das Stilelement, das einem Bereich ein bestimmtes Erscheinungsbild verleiht. Das Portal stellt mehrere Motive bereit, ähnlich Hintergrundbildern, die beim Einrichten eines Bereichs ausgewählt werden können.

Monitoring-Kontextinstanz
Informationen in IBM WebSphere Business Monitor, die zu Überwachungszwecken zu einem bestimmten Zeitpunkt zusammengetragen werden.

O

Oberfläche
Ein Element der grafischen Benutzerschnittstelle, das geändert werden kann, um eine andere Darstellung der Schnittstelle ohne Auswirkung auf die zugehörige Funktionalität zu erzielen.

Ontologie
Eine explizite formale Spezifikation der Darstellung von Objekten, Konzepten und sonstigen Entitäten, die in einem Interessengebiet vorhanden sein können. Außerdem befasst sich die Ontologie mit deren Beziehungen untereinander.

OWL Siehe Web Ontology Language.

P

Personalisierung
Der Prozess, mit dem die Bereitstellung von Informationen gezielt unter Berücksichtigung von Geschäftsregeln und Benutzerprofildaten auf bestimmte Personen zugeschnitten werden kann. Siehe auch Anpassung.

Plug-in
Ein gesondert installierbares Softwaremodul, das die Funktionen von bereits vorhandenen Programmen, Anwendungen oder Schnittstellen erweitert.

PMR Siehe Problem Management Record.

Polygon
In der GDDM-Funktion eine Folge anstoßender gerader Linien, die eine Fläche eingrenzen.

Portal Ein einziger sicherer Zugriffspunkt auf unterschiedliche Informationen, Anwendungen und Personen, der angepasst und personalisiert werden kann.

Portlet
Eine wiederverwendbare Komponente, die Teil einer Webanwendung ist und die Anzeige spezifischer Informationen oder Services im Kontext eines Portals ermöglicht.

Positionskarte
Eine Karte, die interaktive Bereiche enthält, die im IBM Intelligent Operations Center definiert wurden. Ereignisse können einem oder mehrerer dieser Bereiche zugeordnet werden. Ein Schaubild der Sitzgelegenheiten in einem großen Sportstadion kann z. B. so definiert werden, dass Ereignisse, die bereits stattgefunden haben, dem entsprechenden Bereich zugeordnet werden können.

Problem Management Record (PMR)
Die Nummer im Mechanismus von IBM Support, die für einen Servicefall bei einem Kunden steht.

R

RDF Siehe Resource Description Framework.

Really Simple Syndication (RSS)
Ein XML-Dateiformat für syndizierte Webinhalte, das auf der Spezifikation Really Simple Syndication (RSS 2.0) basiert. RSS-XML-Dateiformate werden von Internetnutzern verwendet, um auf einer Website RSS-Feeds zu abonnieren.

Representational State Transfer (REST)
Ein Softwarearchitekturstil für verteilte Hypermediasysteme wie das World Wide Web. Dieser Be-

griff wird auch häufig verwendet, um eine einfache Schnittstelle zu beschreiben, die XML (YAML, JSON oder reinen Text) über HTTP verwendet und dabei ohne eine zusätzliche Messaging-Ebene, wie zum Beispiel SOAP, auskommt.

Resource Description Framework (RDF)
Ein Framework für die Darstellung von Informationen im World Wide Web.

Ressourcenpaket

1. >Eine Klasse, die den Text für Geschäftsseiten enthält. Die Erstellung von Paketdateien und der Zugriff auf diese erfolgt anhand der Java-API PropertyResourceBundle.
2. Eine strukturierte Datensammlung, die eine Schlüssel-Wert-Zuordnung für Daten (Ressourcen) bietet, die beim Lokalisieren eines Programms verwendet werden. Normalerweise sind die Werte Zeichenfolgen, sie können jedoch auch strukturierte Daten sein.

REST Siehe Representational State Transfer.

RSS Siehe Really Simple Syndication.

S

Secure Sockets Layer (SSL)
Sicherheitsprotokoll, das die Vertraulichkeit der Datenübertragung sichert. SSL ermöglicht es Client/Server-Anwendungen, in einer Art und Weise zu kommunizieren, in der Datensicherheit gegeben ist und das Vortäuschen einer anderen Identität sowie das Fälschen von Nachrichten verhindert wird.

Seite In einer Portalumgebung das Schnittstellenelement, das mindestens ein Portlet enthält.

SGML
Siehe Standard Generalized Markup Language.

Single Sign-on (SSO)
Ein Authentifizierungsprozess, bei dem ein Benutzer durch die Eingabe einer einzigen Benutzer-ID mit dem zugehörigen Kennwort auf mehrere Systeme oder Anwendungen zugreifen kann.

SOAP Ein XML-basiertes Lightweight-Protokoll für den Austausch von Informationen in einer dezentralen, verteilten Umgebung. SOAP kann verwendet werden, um über das Internet Informationen abzufragen und zurückzugeben und Services aufzurufen. Siehe auch Web-Services.

SPARQL
Eine Abfragesprache für Datensatzdefinitionsfelder (RDF), die dazu verwendet wird, Fragen in Bezug auf unterschiedliche Datenquellen zu formulieren. Die W3-Spezifikation definiert die Syntax und Semantik der SPARQL-Abfragesprache.

SSL Siehe Secure Sockets Layer.

SSO Siehe Single Sign-on.

Standard Generalized Markup Language (SGML)
Eine auf dem Standard ISO 8879 basierende Standardmetasprache zum Definieren von Auszeichnungssprachen. SGML konzentriert sich nicht auf die Darstellung der Informationen, sondern auf deren Strukturierung; SGML trennt die Struktur und den Inhalt von der Darstellung. Darüber hinaus erleichtert diese Sprache den Austausch von Dokumenten über ein elektronisches Mittel.

Standard Operating Procedure
Eine Prozedur, die eine Aktivitätensequenz definiert, die durch ein Ereignis ausgelöst wird, dessen Parameter bestimmten vordefinierten Bedingungen entsprechen.

Störung
Ein Ereignis, das nicht Teil der Standardausführung eines Service ist und das eine Unterbrechung oder eine Verminderung der Servicequalität und Kundenproduktivität zur Folge hat oder haben kann. Siehe auch Ereignis.

T

Tabelle mit Systemeigenschaften
Eine Tabelle, in der systemweite Konfigurationsdaten für das IBM Intelligent Operations Center erfasst werden.

TAI Siehe Trust-Association-Interceptor.

TCP/IP
Siehe Transmission Control Protocol/Internet Protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP)
Eine standardisierte nicht proprietäre Gruppe von Übertragungsprotokollen, die zuverlässige End-to-End-Verbindungen zwischen Anwendungen über miteinander verbundene Netze unterschiedlichen Typs bereitstellt.

Trigger
Ein Mechanismus, der einen Vorfall erkennt und daraufhin eine weitere Verarbeitung auslösen kann.

Trust-Association-Interceptor (TAI)
Der Mechanismus, mit dem in der Produktumgebung die Anerkennung jeder vom Proxy-Server empfangenen Anforderung geprüft wird. Der Proxy-Server und der Abfangprozess vereinbaren die Prüfmethode.

U

Überprüfter Portalbenutzer
Ein Benutzer, der ein Mitglied einer Interessengruppe innerhalb des WebSphere Portals ist, authentifiziert durch ein Profil, das ein Kennwort und eine Benutzer-ID beinhaltet.

Überwachungsmodell
Ein Modell, das die Aspekte des Geschäftsleistungsmanagements eines Geschäftsmodells beschreibt, wie Ereignisse, Geschäftsmessgrößen und wesentliche Leistungsindikatoren (KPI = Key Performance Indicator), die für die Geschäftsüberwachung in Echtzeit erforderlich sind.

Uniform Resource Identifier (URI)

1. Eine eindeutige Adresse, die zur Bestimmung von Webinhalten, wie z. B. einer Textseite, eines Video- oder Sound-Clips, einer Grafik mit oder ohne Animation oder eines Programms verwendet wird. Die häufigste Form einer URI ist die Adresse einer Webseite, die eine spezielle Form oder ein Subset einer URI ist, genannt Uniform Resource Locator (URL). Eine URI beschreibt üblicherweise, wie auf die Ressource, auf den Computer, der die Ressource enthält, und auf den Namen der Ressource (ein Dateiname) zugegriffen wird.
2. Eine komprimierte Zeichenfolge zur Bestimmung einer abstrakten oder physischen Ressource.

Uniform Resource Locator (URL)
Die eindeutige Adresse einer Informationsressource, auf die in einem Netz, z. B. im Internet, zugegriffen werden kann. Die URL gibt den abgekürzten Namen des Protokolls an, das beim Zugriff auf die Informationsressource verwendet wird, sowie die Informationen, die vom Protokoll bei der Suche nach der Informationsressource verwendet werden.

Unternehmensarchiv (EAR)
Ein besonderer Typ einer JAR-Datei, der durch den Java EE-Standard definiert ist und der zur Implementierung von Java EE-Anwendungen auf Java EE-Anwendungsservern verwendet wird. Eine EAR-Datei enthält EJB-Komponenten, einen Implementierungsdeskriptor sowie Webarchivdateien (WAR-Dateien) für einzelne Webanwendungen. Siehe auch Java-Archiv.

URI Siehe Uniform Resource Identifier.

URL Siehe Uniform Resource Locator.

V

Verkehrsqualität (Level of Service, LOS)
Ein qualitativer Messwert, der im Transportwesen von Verkehrsingenieuren zur Ermittlung der Effektivität von Elementen einer Transportinfrastruktur verwendet wird. Dieser Messwert beschreibt die aktive Verkehrssituation unter Berücksichtigung der Definitionen im Highway Capacity Manual.

Verschachtelter KPI
Ein Key Performance Indicator (KPI), der als untergeordnetes Element eines übergeordneten KPIs definiert ist.

Virtual Network Computing (VNC)
Ein grafisches Desktop-Sharing-System, das das fernbediente Anzeigenpufferprotokoll (RFB) verwendet, um einen anderen Computer fernzusteuern. Es überträgt die Tastatur- und Mausereignisse von einem Computer auf einen anderen, indem es die aktualisierten grafischen Anzeigen über das Netz in die andere Richtung zurück überträgt.

VNC Siehe Virtual Network Computing.

W

Web Map Service (WMS)
Ein Standardprotokoll für die Bereitstellung georeferenzierter Kartengrafiken über das Internet. Diese werden durch einen Kartenserver generiert, der hierfür Daten aus einer GIS-Datenbank verwendet. Die Spezifikation wurde vom Open Geospatial Consortium entwickelt und erstmals im Jahr 1999 veröffentlicht.

Web Ontology Language (OWL)
Eine Sprache, mit der die Bedeutung von Begriffen im jeweiligen Vokabular sowie deren Beziehungen untereinander explizit dargestellt werden. Web Ontology Language sollte verwendet werden, wenn die in Dokumenten enthaltenen Informationen nicht einfach Personen zur Verfügung gestellt, sondern von Anwendungen verarbeitet werden sollen.

Web-Service
Eine eigenständige, selbsterklärende, modulare Anwendung, die mithilfe von standardmäßigen Netzprotokollen in einem Netz veröffentlicht, erkannt und aufgerufen werden kann. Normalerweise wird XML verwendet, um die Daten mit Tags zu versehen, SOAP dient zur Übertragung der Daten, WSDL dient zur Beschreibung der verfügbaren Services und UDDI wird zum Auflisten der verfügbaren Services verwendet. Siehe auch SOAP, Web Service Definition Language.

Web Services Description Language (WSDL)
Eine XML-basierte Spezifikation zur Beschreibung vernetzter Services als eine Gruppe von Endpunkten, die mithilfe von Nachrichten arbeiten, die entweder dokumentorientierte oder verfahrensorientierte Informationen enthalten. Siehe auch Web-Service.

Widget
Eine wiederverwendbare Benutzerschnittstellenkomponente wie beispielsweise eine Schaltfläche, eine Bildlaufleiste, ein Steuerbereich oder ein Textverarbeitungsbereich. Die Eingabe in das Widget kann über die Tastatur oder Maus erfolgen. Ein Widget kann mit einer Anwendung oder anderen Widgets kommunizieren. Siehe auch Allgemeines Widget.

WMS Siehe Web Map Service.

WO Siehe Auftrag.

Workflow
Eine bestimmte Folge von Aktionen, die sich für bestimmte Situationen eignet. Die Lösung kann durch eine entsprechende Anpassung jeweils geeignete Workflows auslösen. So kann beispielsweise eine Verbindung zu Notfallabwehrsystemen hergestellt werden.

WSDL
Siehe Web Service Description Language.

X

XML Siehe Extensible Markup Language.

XML-Schema
Ein Mechanismus zur Beschreibung und Beschränkung des Inhalts von XML-Dateien, indem angezeigt wird, welche Elemente in welcher Kombination zulässig sind. XML-Schemas sind eine Alternative zu Dokumenttypdefinitionen (DTDs) und können dazu verwendet werden, um die Funktionalität im Bereich der Datentypisierung, Vererbung und Darstellung zu erweitern.

Z

Zugriffssteuerungsliste (Access Control List, ACL)
In der IT-Sicherheit ist dies eine Liste, die einem Objekt zugeordnet ist. Sie enthält alle Subjekte, die auf das Objekt zugreifen können, sowie deren Zugriffsberechtigungen.

Zusätzliche Produktinformationen

Die folgenden zusätzlichen Informationen stehen online zur Verfügung.

WebSphere Portal

- Produktunterstützungsseite für WebSphere Portal: http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere_Portal
- Informationsbibliothek für WebSphere Portal: http://www.ibm.com/software/genservers/portal/library/
- Wiki für WebSphere Portal: http://www.lotus.com/ldd/portalwiki.nsf

WebSphere Application Server

- Produktunterstützungsseite für WebSphere Application Server: http://www.ibm.com/software/webservers/appserv/was/support/
- Informationsbibliothek für WebSphere Application Server: http://www.ibm.com/software/webservers/appserv/was/library/index.html
- Information Center für WebSphere Application Server 7.0.x: http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

Information Center

- Information Center für Cognos: http://publib.boulder.ibm.com/infocenter/cbi/v10r1m1/index.jsp
- Information Center für DB2: http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp
- Information Center für IBM ILOG CPLEX Optimization Studio: http://pic.dhe.ibm.com/infocenter/cosinfoc/v12r4/index.jsp
- Information Center für Lotus Domino: http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp
- Information Center für Lotus Notes: http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp
- Information Center für Lotus Sametime Standard: http://publib.boulder.ibm.com/infocenter/sametime/v8r5/index.jsp
- Information Center für Rational Application Developer: http://publib.boulder.ibm.com/infocenter/radhelp/v7r5/index.jsp?topic=/com.ibm.rad.legal.doc/helpindex_rad.html
- Information Center für Tivoli Access Manager: http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml
- Information Center für Tivoli Composite Application Manager: http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp
- Information Center für Tivoli Directory Integrator: http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDI.doc_7.1/welcome.htm
- Information Center für Tivoli Directory Server: http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml
- Information Center für Tivoli Identity Manager : http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml
- Information Center für Tivoli Netcool/Impact: http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcoolimpact.doc5.1.1/welcome.html
- Information Center für Tivoli Netcool/OMNIbus: http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcool_OMNIbus.doc_7.3.1/omnibus/wip/welcome.htm
- Information Center für Tivoli Service Request Manager: http://publib.boulder.ibm.com/infocenter/tivihelp/v32r1/index.jsp?topic=/com.ibm.srm.doc/srm_welcome.htm
- Information Center für IBM WebSphere Business Monitor: http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r0mx/index.jsp?topic=/com.ibm.btools.help.monitor.doc/home/home.html

- Information Center für WebSphere Message Broker: http://publib.boulder.ibm.com/infocenter/wmbhelp/v8r0m0/index.jsp
- Information Center für WebSphere MQ: http://publib.boulder.ibm.com/infocenter/wmqv7/v7r1/index.jsp
- Information Center für WebSphere Operational Decision Management: http://pic.dhe.ibm.com/infocenter/dmanager/v7r5/index.jsp

Redbooks

- Redbooks-Domäne: http://www.redbooks.ibm.com/

Sonstige Webressourcen

- Tivoli-Schulung und -Zertifizierung: http://www.ibm.com/software/tivoli/education/
- OASIS Common Alerting Protocol Version 1.2 http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html
- Red Hat-Website: http://www.redhat.com/

Zugehörige Konzepte:

„Zielgruppe" auf Seite 2
Dieses Information Center richtet sich an Personen, die das IBM Intelligent Operations Center verwenden, installieren, verwalten und pflegen. Es enthält unter anderem auch eine Dokumentation der Implementierung zur Anpassung der Lösung und Integration der externen zugrunde liegenden Systeme, die vom IBM Intelligent Operations Center benötigt werden.

Copyrightvermerk und Marken

Copyrightvermerk

Marken

Cognos, CPLEX, IBM, WebSphere, DB2, Domino, ILOG, Lotus, Notes, Rational, Tivoli, ibm.com, Passport Advantage, Sametime, Service Request Manager, Smarter Cities und Redbooks sind Marken der IBM Corporation in den USA und/oder anderen Ländern.

Microsoft, Internet Explorer, Windows und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Pentium ist eine eingetragene Marke der Intel Corporation oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern.

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

Adobe, Acrobat, Portable Document Format (PDF) und PostScript sind eingetragene Marken oder Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Oracle, JavaScript und Java sind eingetragene Marken von Oracle und/oder den zugehörigen verbundenen Unternehmen.

ArcGIS, EDN, StreetMap, @esri.com und www.esri.com sind Marken, eingetragene Marken oder Servicemarken von Esri in den USA, in der Europäischen Gemeinschaft oder in bestimmten anderen Gerichtsbarkeiten.

Sonstige Namen können Marken der jeweiligen Rechtsinhaber sein. Weitere Unternehmens-, Produkt- und Servicenamen können Marken oder Servicemarken anderer Hersteller sein.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. An Stelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
Department T81B F6/Building 503
4205 S. Miami Boulevard
Durham NC 27709-9990
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis) und ohne jegliche Gewährleistung zur Verfügung gestellt. IBM übernimmt keine Haftung für Schäden, die durch die Verwendung der Beispielprogramme entstehen.

Index

Antwort

IBM Intelligent Operations Center
IBM Intelligent Operations Center
Produktdokumentation
Version 1 Release 5

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen. Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre IBM Geschäftsstelle, Ihren IBM Geschäftspartner oder Ihren Händler.

Unsere Telefonauskunft "HALLO IBM" (Telefonnr.: 0180 3 313233) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.

Kommentare:

Danke für Ihre Bemühungen.

Sie können ihre Kommentare betr. dieser Veröffentlichung wie folgt senden:
- Als Brief an die Postanschrift auf der Rückseite dieses Formulars
- Als E-Mail an die folgende Adresse: translation@de.ibm.com

Name	Adresse
Firma oder Organisation	
Rufnummer	E-Mail-Adresse

Antwort

IBM Deutschland GmbH
TSC Germany

71083 Herrenberg