

IBM Business Monitor



# IBM Business Monitor Installationshandbuch

*Version 8 Release 0*



IBM Business Monitor



# IBM Business Monitor Installationshand- buch

*Version 8 Release 0*



---

# Inhaltsverzeichnis

## Kapitel 1. IBM Business Monitor installieren . . . . . 1

## Kapitel 2. Installation von IBM Business Monitor planen . . . . . 3

Geeignete Topologien auswählen . . . . .	3
Einzelservertopologie . . . . .	3
Topologie für Hochverfügbarkeit (Netzimplementierung) . . . . .	3
Vorhandene Softwarevoraussetzungen nutzen . . . . .	9
Profile . . . . .	10
Profiltyp auswählen . . . . .	10
Hinweise zur Datenbankplanung . . . . .	12
Hinweise zur MONITOR-Datenbank für DB2 . . . . .	14
Hinweise zur Cognos-Datenbank für DB2 . . . . .	16
Hinweise zur MONITOR-Datenbank für DB2 for z/OS . . . . .	18
Hinweise zu Cognos-Datenbanken für DB2 for z/OS . . . . .	20
Hinweise zur MONITOR-Datenbank für Oracle . . . . .	21
Hinweise zur Cognos-Datenbank für Oracle . . . . .	24
Hinweise zur MONITOR-Datenbank für Microsoft SQL Server . . . . .	26
Hinweise zur Cognos-Datenbank für Microsoft SQL Server . . . . .	27
Hinweise zur Benutzerregistry . . . . .	28
Hinweise für Benutzer ohne Verwaltungsaufgaben . . . . .	29
Hinweise zur Topologie . . . . .	30
Hinweise für eine Einzelservertopologie . . . . .	30
Hinweise für eine Network Deployment-Topologie unter Verwendung von Implementierungsumgebungsmustern . . . . .	30
Hinweise für angepasste Network Deployment-Topologie . . . . .	31
Hinweise für IBM Business Process Manager in einer Umgebung mit Vier-Cluster-Topologie . . . . .	32

## Kapitel 3. Installation vorbereiten . . . . . 35

Hardware- und Softwarevoraussetzungen . . . . .	35
Betriebssysteme für die Produktinstallation vorbereiten . . . . .	35
AIX-Systeme für die Installation vorbereiten . . . . .	35
Linux-Systeme für die Installation vorbereiten . . . . .	36
Solaris-Systeme für die Installation vorbereiten . . . . .	39
Windows-Systeme für die Installation vorbereiten . . . . .	40

## Kapitel 4. IBM Business Monitor-Software installieren . . . . . 41

Über das Produkt-Launchpad installieren . . . . .	41
IBM Business Monitor im Dialogbetrieb installieren . . . . .	44
IBM Business Monitor unbeaufsichtigt installieren . . . . .	48
Unbeaufsichtigte Installation von IBM Business Monitor über die Befehlszeile . . . . .	48

Unbeaufsichtigte Installation von IBM Business Monitor mithilfe einer Antwortdatei . . . . .	53
Information Center installieren . . . . .	55
Lokales Information Center starten und stoppen . . . . .	56
Lokales Information Center aktualisieren . . . . .	56

## Kapitel 5. Datenbanken erstellen. . . . . 59

Datenbankskripts mit dem Datenbankentwurfstool erstellen oder konfigurieren . . . . .	61
MONITOR-Datenbankskripts manuell konfigurieren . . . . .	62
COGNOSCS-Datenbankskripts manuell konfigurieren . . . . .	66
Monitor-Datenbank manuell installieren . . . . .	67
COGNOSCS-Datenbank manuell installieren . . . . .	69
Tabellen für Messaging-Steuerkomponente manuell erstellen . . . . .	70
Skripts für die Erstellung von Datenbankobjekten in DB2 für z/OS generieren . . . . .	71
Datenbanken im DB2 for z/OS-Subsystem erstellen . . . . .	73
Aliasnamensdefinitionen für die Verbindung zum DB2 für z/OS-Server einrichten . . . . .	74
DB2 für z/OS-Datenbankobjekte mit dem Script 'createDB2.sh' erstellen . . . . .	75
DB2 für z/OS-Datenbankobjekte über den DB2-Befehlszeilenprozessor erstellen . . . . .	77
Hinweise zur Einrichtung und Konfiguration von High Availability Disaster Recovery (HADR) . . . . .	80
Oracle Real Application Cluster (RAC) zur Verwendung mit IBM Business Monitor konfigurieren . . . . .	82
Oracle Data Guard für IBM Business Monitor konfigurieren . . . . .	83

## Kapitel 6. Profile erstellen und erweitern . . . . . 87

Profile mit dem Profile Management Tool erstellen und erweitern . . . . .	87
Eigenständige Profile erstellen . . . . .	88
Deployment Manager-Profil erstellen . . . . .	96
Deployment Manager-Profil erweitern . . . . .	103
Angepasste Profile für Knoten erstellen . . . . .	109
Angepasste Profile für Knoten erweitern . . . . .	112
Profile mit dem Befehl 'manageprofiles' erstellen und erweitern . . . . .	114

## Kapitel 7. Installation überprüfen . . . . . 117

## Kapitel 8. Portnummern ermitteln . . . . . 119

## Kapitel 9. Umgebung konfigurieren . . . . . 121

Implementierungsumgebung mit einem Muster erstellen . . . . .	121
Auf Gestaltungsdokumenten basierende Implementierungsumgebungsdefinitionen importieren . . . . .	129

IBM Business Monitor-Implementierungsumgebung einer IBM Business Process Manager-Serverimplementierungsumgebung hinzufügen . . . . .	137
Die Implementierungsumgebung mithilfe einer benutzerdefinierte Topologie erstellen . . . . .	139
IBM Business Monitor-Cluster erstellen. . . . .	139
CEI-Ereignisservices konfigurieren . . . . .	142
Umgebung mit dem Konfigurationsassistenten konfigurieren . . . . .	143
Umgebung mithilfe von wsadmin-Befehlen konfigurieren. . . . .	150
Umgebung manuell konfigurieren . . . . .	152

**Kapitel 10. IBM Business Monitor-Komponenten konfigurieren . . . . . 167**

IBM Cognos BI konfigurieren . . . . .	167
Neuen IBM Cognos BI-Service konfigurieren	167
IBM Business Monitor und Business Space für die Verwendung eines vorhandenen IBM Cognos BI-Service konfigurieren . . . . .	172
IBM Cognos BI mit WebSphere Portal konfigurieren . . . . .	174
Berichtsdatenquelle in IBM Cognos BI konfigurieren . . . . .	176
IBM Business Monitor-Widgets für WebSphere Portal konfigurieren . . . . .	177
Empfang von Ereignissen konfigurieren . . . . .	177
Hinweise zu asynchronen Ereignissen . . . . .	177
Ereignisse von der CEI empfangen . . . . .	179
Business Space konfigurieren . . . . .	187

Business Space konfigurieren . . . . .	187
Globales Prozess-Monitormodell konfigurieren . . . . .	355
Globales Prozess-Monitormodell manuell installieren . . . . .	355
Ereignisse für das globale Prozess-Monitormodell aktivieren . . . . .	356
Dashboards für das globale Prozess-Monitormodell konfigurieren . . . . .	357

**Kapitel 11. Präsentationsmodell installieren . . . . . 359**

**Kapitel 12. IBM Business Monitor aktualisieren. . . . . 361**

IBM Cognos BI aktualisieren . . . . .	361
Fixpacks und vorläufige Fixes im Dialogbetrieb installieren . . . . .	362
Fixpacks unbeaufsichtigt installieren. . . . .	365
Vorläufige Fixes unbeaufsichtigt installieren . . . . .	366
Rollback eines Fixpacks durchführen . . . . .	367
Vorläufige Fixes im Dialogbetrieb deinstallieren	368
Vorläufige Fixes unbeaufsichtigt deinstallieren . . . . .	369

**Kapitel 13. IBM Business Monitor deinstallieren . . . . . 371**

IBM Business Monitor interaktiv deinstallieren . . . . .	371
IBM Business Monitor unbeaufsichtigt deinstallieren . . . . .	372
Präsentationsmodell entfernen. . . . .	373

---

## Kapitel 1. IBM Business Monitor installieren

IBM® Business Monitor kann in verschiedenen Topologien installiert werden. Sie können alle Komponenten auf ein und demselben Server installieren oder die Komponenten auf mehrere Systeme verteilen. Zur Realisierung einer hoch verfügbaren Umgebung mit Failoverunterstützung können Sie IBM Business Monitor in einer Clusterumgebung installieren, in der der Clusteringmechanismus von WebSphere Application Server oder Process Server genutzt wird.

**Wichtig:** IBM Business Monitor kann auf verschiedenen Plattformen ausgeführt werden. Details zu den unterstützten Betriebssystemen, unterstützter Hardware, Speicherbedarf und erforderlichem Plattenspeicherplatz finden Sie unter den Systemanforderungen für IBM Business Monitor.





---

## Kapitel 2. Installation von IBM Business Monitor planen

IBM Business Monitor setzt sich aus verschiedenen Komponenten zusammen, die auf einem einzigen Server oder verteilt auf mehreren Servern im Netz installiert werden können. Während des Installationsprozesses müssen zahlreiche Optionen in Betracht gezogen werden. Bei der Planung der Installation von IBM Business Monitor müssen Sie die verfügbaren Optionen berücksichtigen und festlegen, wie die Komponenten in Ihrem Netz eingesetzt werden sollen.

Die bereitgestellten Informationen helfen Ihnen bei der Entscheidung, welche Topologie sich für Ihre Umgebung am besten eignet, und erläutern die Optionen, die während der Installation zur Auswahl stehen.

Lesen Sie die folgenden Informationen, bevor Sie mit der Installation von IBM Business Monitor beginnen:

---

### Geeignete Topologien auswählen

IBM Business Monitor kann in vielen verschiedenen Konfigurationen installiert werden. Einige grundlegende Topologien werden bereitgestellt. Diese müssen Sie gegebenenfalls an die jeweilige Umgebung anpassen.

Die folgenden Topologien veranschaulichen einige allgemeine Installationen. Sie können auf diese Weise einige mögliche Installationsverteilungen kennen lernen:

#### Einzelservertopologie

Wenn Sie eine Einzelservertopologie verwenden, werden alle unterstützenden Produkte und alle IBM Business Monitor-Komponenten auf demselben physischen Server installiert.

Die Einzelserverinstallation von IBM Business Monitor eignet sich besonders für Entwicklungstestumgebungen, für Konzeptnachweisumgebungen und für einfache Implementierungen, die keine Funktionen für Funktionsübernahme und hohe Verfügbarkeit erfordern.

Mit dem IBM Business Monitor-Installationsprogramm können Sie IBM Business Monitor und WebSphere Application Server installieren. Wenn Sie IBM Business Monitor auf einem einzelnen Server installieren, dann wird der Cognos-Service ebenfalls installiert. Zum Anzeigen der überwachten Daten können Sie entweder ein Business Space-Dashboard oder ein portletbasiertes Dashboard verwenden.

Nach der Installation von IBM Business Monitor müssen Sie ein eigenständiges Profil erstellen, um Ihre Laufzeitumgebung zu definieren. Wenn Sie ein eigenständiges Profil erstellen oder erweitern, werden alle erforderlichen IBM Business Monitor-Komponenten erstellt.

#### Topologie für Hochverfügbarkeit (Netzimplementierung)

IBM Business Monitor verwendet die Hochverfügbarkeitsfunktionen in WebSphere Application Server oder in Process Server-Network Deployment-Umgebungen. Die Netzimplementierung gewährleistet die Kapazität, Skalierbarkeit und Zuverlässigkeit, die in einer Produktionsumgebung generell verlangt wird. In Network Deployment-Umgebungen kann eine Gruppe von Servern gemeinsam eingesetzt wer-

den, um die erforderliche Lastverteilung und Funktionsübernahme bereitzustellen. Die Server werden von einer einzigen Administrationskonsole aus zentral verwaltet.

IBM Business Monitor verwendet dasselbe Architekturmodell wie WebSphere Application Server und Process Server. Mit diesem Modell können Sie Umgebungen mit Zellen, Knoten und Servern und optional auch mit Clustern erstellen.

Wenn Sie eines der verfügbaren Implementierungsumgebungsmuster (Ein-Cluster- oder Vier-Cluster-Muster) auswählen, hilft Ihnen der Implementierungsumgebungsassistent bei der Konfiguration der Cluster, Server und Komponenten, die Sie benötigen.

Die Hauptverwaltungsdomäne ist die Zelle. Sie können sich eine Zelle als eine logische Gruppierung von Servern oder Clustern oder eine Kombination aus beiden vorstellen. (Ein Cluster ist eine Gruppe aus Anwendungsservern, die zum Zwecke der Lastverteilung und Funktionsübernahme zusammenarbeiten.) Mit Servern und Clustern können Sie IBM Business Monitor in einer einzigen Zelle installieren, die sich durch Hochverfügbarkeit und Skalierbarkeit auszeichnet.

Ein verwalteter Knoten (ein Knoten in einer Zelle) enthält einen oder mehrere Server. Jeder Server stellt eine Laufzeitumgebung bereit. Verwaltete Server werden innerhalb eines verwalteten Knotens erstellt, der über ein angepasstes Profil definiert wird. Jeder der verwalteten Knoten ist in denselben Deployment Manager eingebunden und der Deployment Manager verwaltet alle verwalteten Knoten in der Zelle. Server können in Clustern zusammengefasst werden, die ebenfalls vom Deployment Manager verwaltet werden. In einer Network Deployment-Umgebung sollten Sie die Anwendungen in einem Cluster installieren, sodass die Anwendungen gegen den Ausfall eines einzelnen Servers geschützt sind (hohe Verfügbarkeit) und/oder die Auslastung durch die Anwendungen auf mehrere gleichwertige Server verteilt ist (Lastverteilung).

Weitere Informationen zur Hochverfügbarkeit finden Sie unter 'Hohe Verfügbarkeit und Lastausgleich' in den zugehörigen Links.

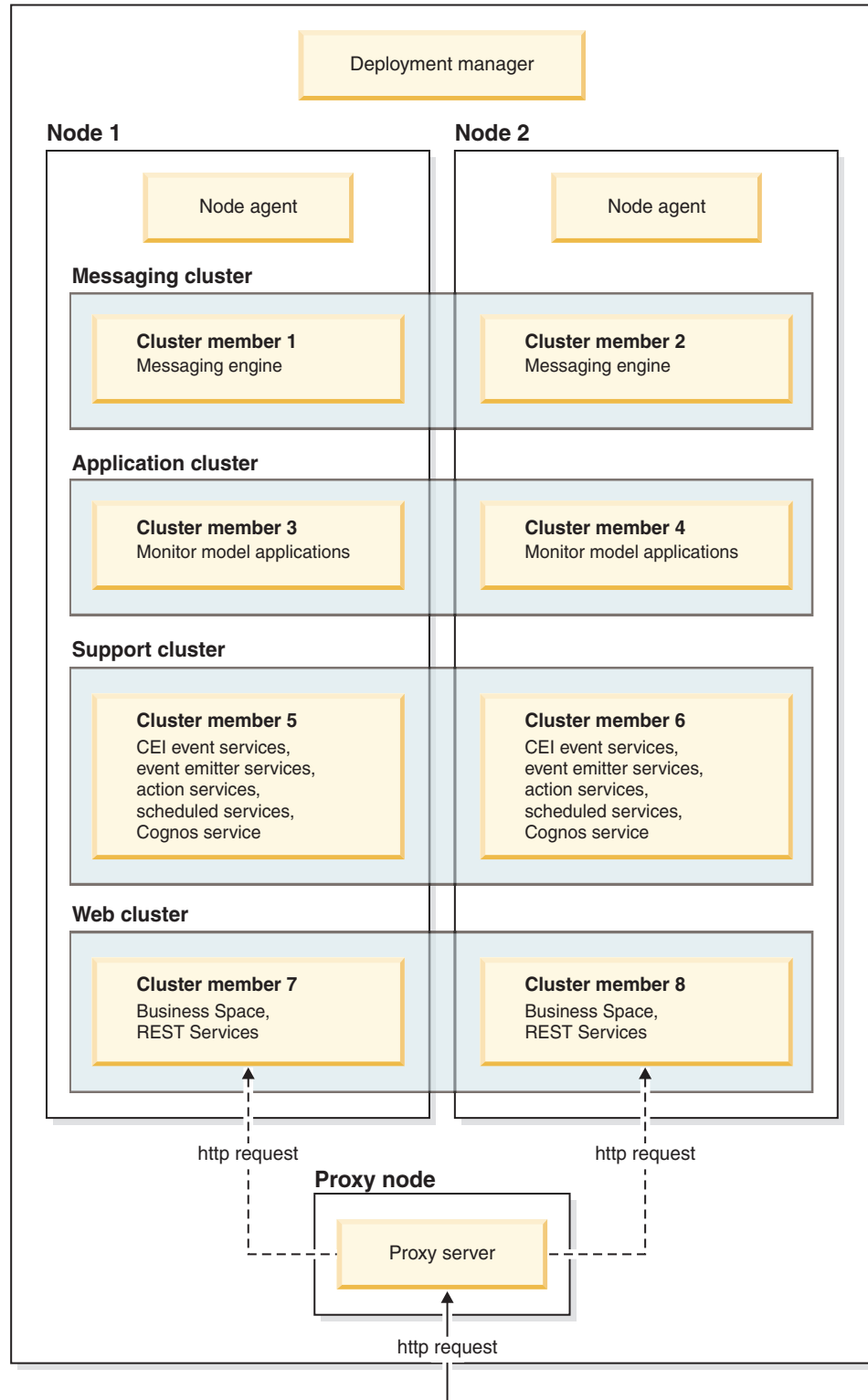
In einer ND-Umgebung wird aus Sicherheitsgründen und zum Zwecke des Lastausgleichs normalerweise ein Proxy-Server oder ein HTTP-Server konfiguriert. Weitere Informationen zum Proxy-Server finden Sie unter dem Thema 'Skalierbarkeit'.

### **Skalierbarkeit**

Installation von IBM Business Monitor-Komponenten und Monitormodellen in einem Cluster ermöglicht eine bessere Verwaltung ihrer Auslastung. Die Verteilung der Komponenten und Monitormodelle über mehrere Cluster und die Gruppierung der Komponenten auf Grundlage allgemeiner Ressourcennutzungsmuster ermöglicht Ihnen, die individuelle Auslastung der einzelnen Cluster basierend auf den Ressourcennutzungsmustern der installierten Komponenten zu verwalten. Einen Vorschlag zum Ausgangspunkt einer skalierbaren Topologie finden Sie im Abschnitt 'Vier-Cluster-Topologie'.

Das folgende Diagramm zeigt eine Zelle mit zwei verwalteten Knoten.

## Cell



## Messaging-Steuerkomponenten

Bei der Implementierung in einem Cluster ist die Messaging-Steuerkomponente, die für den Service Integration Bus von IBM Business Monitor erstellt wurde, jeweils nur in einem Cluster-Member zur Zeit aktiv. Dieses Verhalten wird durch die

Standardrichtlinie des Service Integration Bus angegeben. Während die Standardrichtlinie des Service Integration Bus angepasst werden kann, muss die Richtlinie stets den Typ 'Eins-von-N' aufweisen. Eine 'Eins-von-N'-Richtlinie erlaubt nur eine aktive Instanz der Messaging-Steuerkomponente in einem Cluster. Auf diese Weise wird eine hohe Verfügbarkeit (Schutz der Komponenten und Modelle vor dem Fehlschlagen eines einzelnen Servers) jedoch keine Skalierbarkeit (Erweiterungsmöglichkeit beim Hinzufügen von Ressourcen) erreicht.

Sie können die Verwendung der Messaging-Steuerkomponente minimieren und die Leistung verbessern, indem Sie das Feature verwenden, das dem CEI-Ereignis-service eine Umgehung der JMS-Warteschlangen (JMS, Java Messaging Service) und die direkte Übergabe von Ereignissen an die IBM Business Monitor-Datenbank ermöglicht. Weitere Informationen finden Sie unter "Ereignisse mithilfe der tabellenbasierten Ereigniszustellung empfangen" in den zugehörigen Tasklinks.

### **Komponenten unterstützen**

Die Unterstützungskomponenten umfassen den CEI-Ereignis-service, den IBM Cognos Business Intelligence-Service, die Aktionsservices und Ereignis-Emitter-Services sowie die geplanten Services. Fügen Sie bei erhöhtem Nutzungsvolumen neue Cluster-Member hinzu. Dies gilt jedoch nicht für geplante Services.

Die größte Arbeitslast für geplante Services tritt auf dem Datenbankserver auf. Wenn die Arbeitslast für geplante Services steigt, sollten Sie den Datenbankserver überwachen, bewerten und bei Bedarf optimieren. Die Arbeitslast der geplanten Services kann auch durch die Aktivierung oder Inaktivierung verschiedener geplanter Services oder durch Bearbeitung des Serviceintervalls verwaltet werden, das den einzelnen geplanten Services zugeordnet ist. Weitere Informationen finden Sie im Abschnitt "Geplante Monitor-Services verwalten" in den zugehörigen Tasklinks.

### **Webkomponenten**

Webkomponenten umfassen Business Space, Widgets und den REST-API-Service von IBM Business Monitor. Fügen Sie bei erhöhtem Nutzungsvolumen neue Cluster-Member hinzu.

In einer ND-Umgebung wird aus Sicherheitsgründen und zum Zwecke des Lastausgleichs normalerweise ein Proxy-Server oder ein HTTP-Server konfiguriert. Eingehende HTTP-Anforderungen werden nicht direkt an einen WebSphere Application Server sondern an einen Proxy-Server weitergeleitet, der die Anforderungen auf mehrere Anwendungsserver verteilen kann, die die Verarbeitung durchführen. Erstellen Sie einen Proxy-Server in WebSphere Application Server. Sie können anstelle des Proxy-Servers oder vor dem Proxy-Server weitere Routing-Server verwenden, z. B. IBM HTTP Server. Der Proxy-Server hat den Vorteil, dass er in WebSphere Application Server integriert und deshalb einfach zu verwenden und zu verwalten ist.

**Wichtig:** Für den Lastausgleich von HTTP-Anforderungen zwischen zwei oder mehr Cluster-Memberrn ist der Proxy-Server (oder ein alternativer Routing-Server) erforderlich. Der Proxy-Server ermöglicht Clients den Zugriff auf die Anwendungen innerhalb dieser Topologie.

## Monitormodellanwendungen

Monitormodellanwendungen sind als Standard-Java-EAR-Dateien gepackt (EAR, Enterprise Application Archives). Die Monitormodellanwendung passt sich in der Größe nach an, je nachdem wie viele Cluster-Member sich im Cluster befinden.

## Hinweis zum Hauptspeicher

Die Menge des verfügbaren Hauptspeichers für ein einzelnes Cluster-Member hängt von der Adressraumbelugung des Betriebssystems ab und davon, ob die ausführende JVM ein 32-Bit-Prozess oder ein 64-Bit-Prozess ist. Während eine 64-Bit-JVM auf eine beliebige Position von 500 GB bis 4 GB des Speichers zugreifen kann, kann eine 32-Bit-JVM möglicherweise nur auf lediglich 2 GB des Hauptspeichers zugreifen (zum Beispiel bei einem 32-Bit-Windows-System).

Als allgemeine Richtlinie empfiehlt sich das Hinzufügen eines zweiten Clusters zur Implementierung von Monitormodellanwendungen, wenn die Implementierung von mehr als zehn Monitormodellanwendungen geplant ist oder wenn die Cluster-Member auf einer 32-Bit-JVM ausgeführt werden. Dies ist jedoch nur eine allgemeine Richtlinie, da einzelne Auslastungen und Modelle erheblich variieren können.

## Vier-Cluster-Topologie

Sie können IBM Business Monitor in viele Topologien installieren. Mit der Vier-Cluster-Topologie können Sie eine Hochleistungsumgebung einrichten.

Die im Folgenden beschriebene Vier-Cluster-Topologie basiert auf dem Muster 'Fernes Messaging, Fernunterstützung und Webimplementierungsumgebung'. In diesem Muster bilden die IBM Business Monitor-Anwendungen Gruppen in Form von vier Clustern in einer einzelnen Zelle.

### Messaging Engine Cluster

WebSphere Business Monitor and CEI buses

### Support Cluster

CEI event services, action services, services scheduler, event emitter services, Cognos service

### Application Cluster

Monitor model applications

### Web Cluster

Business Space application, Business Space widgets, REST services application

## Cluster für Messaging-Steuerkomponente

Messaging-Steuerkomponente für den IBM Business Monitor-Bus

Messaging-Steuerkomponente für den CEI-Bus (Common Event Infrastructure)

### **Unterstützungscluster**

- CEI-Ereignisservice
- Ereignis-Emitter-Services
- Aktionsservices
- geplante Monitor-Services
- IBM Cognos Business Intelligence-Service

### **Anwendungscluster**

- Monitormodellanwendungen

### **Web-Cluster**

- Business Space-Anwendung
- Business Space-Widgets
- Anwendung für REST-Services (Representational State Transfer)

**Anmerkung:** Ordnen Sie die Ereignis-Emitter-Services und den CEI-Ereignisservice im selben Cluster an, um eine bessere Leistung zu erzielen. Zu den Ereignis-Emitter-Services gehört der REST-Ereignis-Emitter und der JMS-Ereignis-Emitter.

### **Zugehörige Tasks:**

„Hinweise für IBM Business Process Manager in einer Umgebung mit Vier-Cluster-Topologie“ auf Seite 32

Sie können eine Vier-Cluster-Topologie mit IBM Business Process Manager konfigurieren, um eine kombinierte Implementierungsumgebung mit IBM® Business Process Manager und IBM Business Monitor nach dem (aus vier Clustern bestehenden) Muster 'Fernes Messaging, Fernunterstützung und Webanwendungen' zu erstellen. Da eine IBM Business Monitor-Implementierungsumgebung alle Anwendungen in der Zelle überwachen kann, sollten Sie nur eine IBM Business Monitor-Implementierungsumgebung in einer Zelle erstellen. Die Vier-Cluster-Topologie kombiniert IBM Business Monitor-Cluster und Cluster für die IBM Business Process Manager-Messaging-Steuerkomponente zu einem einzigen Cluster.

### **Vier-Cluster-Topologie mit IBM Business Process Manager**

Sie können eine kombinierte Implementierungsumgebung mit IBM Business Process Manager und IBM Business Monitor nach dem (aus vier Clustern bestehenden) Muster 'Fernes Messaging, Fernunterstützung und Webanwendungen' erstellen. Da eine IBM Business Monitor-Implementierungsumgebung alle Anwendungen in der Zelle überwachen kann, sollten Sie nur eine IBM Business Monitor-Implementierungsumgebung in einer Zelle erstellen.

Die Vier-Cluster-Topologie kombiniert IBM Business Monitor und Cluster für die IBM Business Process Manager-Messaging-Steuerkomponente in einem einzigen Cluster. Die im Folgenden beschriebene Vier-Cluster-Topologie basiert auf dem Muster 'Fernes Messaging, Fernunterstützung und Webimplementierungsumgebung'.

### **Cluster für Messaging-Steuerkomponente**

- Messaging-Steuerkomponente für den IBM Business Monitor-Bus
- Messaging-Steuerkomponente für den CEI-Bus (Common Event Infrastructure)
- Messaging-Steuerkomponente für den Process Server-Bus
- Messaging-Steuerkomponente für den Performance Data Warehouse-Bus

(Nur BPM Advanced) Messaging-Steuerkomponente für den SCA-Bus (Service Component Architecture)

(Nur BPM Advanced) Messaging-Steuerkomponente für den BPEL-Bus (Business Process Execution Language)

#### **Unterstützungscluster**

CEI-Ereignisservice

Ereignis-Emitter-Services

Aktionsservices

geplante Monitor-Services

IBM Cognos Business Intelligence-Service

Performance Data Warehouse

(BPM Advanced only) Business Rules Manager

#### **Anwendungscluster**

Monitormodellanwendungen

Prozessanwendungen

(Nur BPM Advanced) BPEL-Anwendungen

#### **Web-Cluster**

Business Space-Anwendung

Business Space-Widgets

Anwendung für REST-Services (Representational State Transfer)

(Nur BPM Advanced) Business Process Choreographer-Tools

## **Vorhandene Softwarevoraussetzungen nutzen**

Sie können IBM Business Monitor auf Servern installieren, auf denen die vorausgesetzte Software bereits installiert ist.

### **Vorhandene Anwendungsserver**

Sie können den IBM Business Monitor Server auf einem physischen Server installieren, auf dem bereits eine Anwendungsserverplattform installiert ist. Die folgenden Anwendungsserverplattformen für IBM Business Monitor werden unterstützt:

- WebSphere Application Server
- Process Server
- WebSphere Enterprise Service Bus

Sie können ein vorhandenes Profil erweitern oder ein neues Profil erstellen, das den IBM Business Monitor Server enthält.

### **Vorhandene Installation von WebSphere Portal**

IBM Business Monitor stellt keine portletbasierten Dashboards mehr zur Verfügung. Allerdings können Ihre IBM Business Monitor-Widgets in WebSphere Portal weiterhin angezeigt werden. Weitere Informationen hierzu erhalten Sie über den Link der zugehörigen Task.



---

## Profile

Ein Profil definiert die Laufzeitumgebung und umfasst alle Dateien, die der Server in der Laufzeitumgebung verarbeitet. In einer Hochverfügbarkeitsumgebung benötigen Sie mehrere Profile, um der Komplexität des Systems gerecht zu werden. Sie können entweder neue Profile erstellen oder vorhandene Profile erweitern.

IBM Business Monitor verfügt über Profilvorlagen zur Aktivierung von Funktionen, die für IBM Business Monitor spezifisch sind. Nach der Installation des Produkts können Sie entweder mit dem Profile Management Tool (in WebSphere Customization Toolbox) oder dem Befehl 'manageprofiles' Profile erstellen oder erweitern. (Bei Verwendung der 64-Bit-Version von IBM Business Monitor müssen Sie den Befehl 'manageprofiles' verwenden.)

Die IBM Business Monitor-Profiltypen sind eine Erweiterung der ähnlich benannten Profiltypen von WebSphere Application Server. Die Profiltypen von IBM Business Monitor stimmen nicht mit den Profiltypen von WebSphere Application Server überein.

Die Verwendung neuer Profile ist effizienter und weniger fehleranfällig als eine mehrfache Installation des Produkts. Entwickler können getrennte Profile für Entwicklung und Test verwenden. Die Verwendung von Profilen anstelle mehrfacher Produktinstallationen bietet folgende Vorteile:

- Sie müssen nur eine einzige Gruppe von Basisproduktdateien pflegen.
- Sie sparen Plattenspeicherplatz.
- Sie können das Produkt einfacher aktualisieren.

### Profiltyp auswählen

Ein Profil definiert eine eindeutige Laufzeitumgebung mit separaten Befehlsdateien, Konfigurationsdateien und Protokolldateien. Profile definieren drei unterschiedliche Umgebungstypen: eigenständiger Einzelserver, Deployment Manager und verwalteter Knoten. Mithilfe von Profilen können Sie mehrere Laufzeitumgebungen auf einem System einrichten, ohne mehrere Kopien des Produkts installieren zu müssen.

Bei einer Einzelserverumgebung muss ein eigenständiges Profil erstellt werden.

Führen Sie bei einer Network Deployment-Umgebung die folgenden Schritte aus:

1. Erstellen Sie das Deployment Manager-Profil vor der Erstellung anderer Profile. Wenn Sie vor der Installation von IBM Business Monitor (z. B. für WebSphere Application Server oder Process Server) ein Deployment Manager-Profil erstellt haben und dasselbe Deployment Manager-Profil für die Verwaltung der IBM Business Monitor-Knoten verwenden möchten, müssen Sie das Profil mithilfe der von IBM Business Monitor bereitgestellten Vorlage erweitern.
2. Erstellen Sie für jeden Knoten, der zum Server-Cluster hinzugefügt werden soll, ein angepasstes Profil. Erweitern Sie alternativ für jeden Knoten, der hinzugefügt werden soll, ein bereits vorhandenes angepasstes Profil.

**Anmerkung:** Wenn der Datenbankserver mehrere installierte Versionen von DB2 oder mehrere DB2-Instanzen enthält, wird bei der Profilerstellung die DB2-Standardversion oder -instanz des Servers verwendet. Gehen Sie nach der Vorgehensweise 'Datenbank manuell installieren' vor, um zu steuern, welche DB2-Version oder -Instanz verwendet wird. So kann der Datenbankadministrator die Verwendung der korrekten Version oder Instanz sicherstellen.



Vorlagen für die einzelnen Profile befinden sich im Verzeichnis `app_server_root/profileTemplates`. Folgende Profilverlagen sind verfügbar:

Profil	Wann zu verwenden
Eigenständiger Monitor Server	Für IBM Business Monitor-Einzelserverumgebungen
Monitor Server Deployment Manager	Wenn Sie eine Network Deployment-Umgebung einrichten, erstellen oder erweitern Sie zuerst dieses Profil. Wenn Sie einen Deployment Manager vor der Installation von IBM Business Monitor erstellt haben und planen, dasselbe Deployment Manager-Profil zur Verwaltung von IBM Business Monitor-Knoten zu verwenden, erweitern Sie das Profil mithilfe der von IBM Business Monitor bereitgestellten Vorlage.
Angepasstes Monitor Server-Profil	Wenn Sie eine Network Deployment-Umgebung einrichten, erstellen oder erweitern Sie angepasste Knoten und installieren Sie später über die Administrationskonsole bestimmte Anwendungen auf den einzelnen angepassten Knoten.

### Eigenständige Profile

Verwenden Sie für IBM Business Monitor für Einzelserverumgebungen ein eigenständiges Profil (sog. eigenständiges Anwendungsserverprofil).

Jeder eigenständige Anwendungsserverknoten verfügt über eine eigene Administrationskonsole, über die Sie den Knoten verwalten können. Ein eigenständiger Knoten kann mehrere Server einschließen.

Ein eigenständiger Server kann ohne großen Aufwand eingerichtet werden und besitzt eine Einstiegskonsole, über die Sie den Server starten und stoppen sowie das Präsentationsbeispiel installieren können. Wenn Sie das Beispiel auf dem eigenständigen Server installieren, können Sie die für das Beispiel verwendeten Ressourcen in der Administrationskonsole anzeigen.

Sie können eigene Lösungen auf dem eigenständigen Server implementieren, aber ein eigenständiger Server kann nicht die Kapazität, Skalierbarkeit und Zuverlässigkeit bieten, die grundsätzlich in einer Produktionsumgebung gefordert werden. Es wird empfohlen, für die Produktionsumgebung eine Network Deployment-Umgebung zu verwenden.

### Deployment Manager-Profil

Bei einem Deployment Manager handelt es sich um einen Server, der Operationen für eine logische Gruppe, eine Zelle oder andere Server steuert. In Network Deployment-Umgebungen wird eine Gruppe von Servern gemeinsam eingesetzt, um Lastausgleich und Funktionsübernahme bereitzustellen. Der Deployment Manager ist die zentrale Stelle für die Verwaltung der Server und Cluster in der Zelle.

Beim Erstellen einer Implementierungsumgebung ist das Deployment Manager-Profil das erste Profil, das erstellt oder erweitert wird. Der Deployment Manager verfügt über eine Einstiegskonsole, über die Sie den Deployment Manager starten und stoppen und seine Administrationskonsole starten können. Über die Administrationskonsole des Deployment Managers können Sie die Server und Cluster in der Zelle verwalten. Dies schließt die Konfiguration von Servern und Cluster, das Hin-

zufügen von Servern zu Clustern, das Starten und Stoppen von Servern und Clustern sowie die Implementierung von Modulen auf den Servern und Clustern ein.

Obwohl der Deployment Manager auch ein Server ist, können Sie keine Module auf dem Deployment Manager selbst implementieren.

Nachdem Sie den Deployment Manager für IBM Business Monitor in einer Network Deployment-Umgebung erstellt oder erweitert haben, können Sie angepasste Knoten erstellen oder erweitern und in den Deployment Manager einbinden oder als Teil des Deployment Managers definieren, um eine Zelle, eine Gruppe von Knoten oder Cluster zu erstellen, die zentral verwaltet werden.

Erstellen oder erweitern Sie das Deployment Manager-Profil vor der Erstellung oder Erweiterung angepasster Profile. Wenn Sie ein Deployment Manager-Profil vor der Installation von IBM Business Monitor erstellt haben und planen, dasselbe Deployment Manager-Profil zur Verwaltung von IBM Business Monitor-Knoten zu verwenden, erweitern Sie das Profil mithilfe der von IBM Business Monitor bereitgestellten Vorlage.

### **Angepasste Profile**

Um eine Network Deployment-Umgebung für IBM Business Monitor zu konfigurieren, können Sie angepasste Knoten erstellen und in die Deployment Manager-Zelle einbinden, in der sie dann verwaltet werden. Alternativ können Sie ein bestehendes angepasstes Profil für jeden Knoten erweitern, den Sie zur Zelle hinzufügen wollen. Später können Sie über die Administrationskonsole bestimmte Anwendungen auf den verschiedenen angepassten Knoten installieren.

Bei einem angepassten Profil handelt es sich um einen leeren Knoten, der nicht wie ein Profil für einen eigenständigen Server die Standardanwendungen oder den Standardserver enthält. Bei der Erstellung oder Erweiterung eines angepassten Profils binden Sie den Knoten ein, um das Deployment Manager-Profil zu identifizieren, das Sie zum Verwalten des Knotens verwenden wollen. Nachdem das angepasste Profil in den Deployment Manager eingebunden wurde, wird der Knoten zu einem *verwalteten Knoten*.

Ein verwalteter Knoten enthält einen Knotenagenten und kann verwaltete Server enthalten. In einem verwalteten Knoten können Sie verwaltete Server konfigurieren und ausführen. Die Server, die in einem verwalteten Knoten konfiguriert sind, bilden die Ressourcen der Implementierungsumgebung. Diese Server werden über die Administrationskonsole des Deployment Managers erstellt, konfiguriert, gestartet, gestoppt, verwaltet und gelöscht. Prozesse im verwalteten Knoten können Cluster-Member einschließen, mit deren Hilfe der Deployment Manager die Arbeitslast für besonders stark genutzte Anwendungen verteilen kann.

Ein verwalteter Knoten kann einen oder mehrere Server enthalten, die von einem Deployment Manager verwaltet werden. Sie können Lösungen auf den Servern in einem verwalteten Knoten implementieren, aber der verwaltete Knoten besitzt keine eigene Administrationskonsole. Der verwaltete Knoten wird durch ein angepasstes Profil definiert und verfügt über eine Einstiegskonsole.

---

## **Hinweise zur Datenbankplanung**

Die Monitor-Hauptdatenbank speichert die IBM Business Monitor-Konfiguration, die Metadaten des Monitor-Modells und die überwachten Daten. Die IBM Cognos Business Intelligence-Konfiguration ist in einer separaten IBM Cognos BI-Content-Store-Datenbank mit dem Namen COGNOSCS gespeichert. Bei der Profilerstellung

wird davon ausgegangen, dass sowohl die Datenbank MONITOR als auch die Datenbank COGNOSCS in derselben Datenbankinstanz erstellt werden.

Für die Datenbanken MONITOR und COGNOSCS können Sie einen allgemeinen Datenbankbenutzernamen verwenden. Möglicherweise empfiehlt sich jedoch die Verwendung getrennter Namen, da IBM Cognos BI beim erstmaligen Starten von IBM Cognos BI seine eigenen Content-Store-Tabellen im Schema des angegebenen Datenbanknamens erstellt.

Die Datenbank MONITOR wird während der Erstellung eigenständiger Profile außerdem auch zum Speichern von Schemata für die folgenden Komponenten verwendet:

- Business Space
- Nachrichtenspeicher für CEI-Messaging-Steuerkomponente
- Nachrichtenspeicher für die IBM Business Monitor-Messaging-Steuerkomponente

Wenn Sie kein eigenständiges Profil verwenden, können Sie dieselbe Datenbank oder verschiedene Datenbanken für diese Komponenten und zusätzlich auch für den CEI-Datenspeicher verwenden, der nicht erforderlich ist und daher nicht standardmäßig erstellt bzw. aktiviert wird.

Für Produktionsumgebungen können Sie aus folgenden unterstützten Datenbankprodukten auswählen:

- DB2
- DB2 for z/OS
- Oracle
- Microsoft SQL Server

In der Monitor-Datenbank werden verschiedene Datentypen gespeichert. Wenn Sie das IBM Business Monitor-Profil erstellen oder die Datenbankskripts ausführen, erstellen Sie Datenbanktabellen, die Konfigurationsdaten für IBM Business Monitor enthalten. Nach der Installation der einzelnen Monitor-Modelle werden weitere Tabellen erstellt, um Daten für diese Monitor-Modelle zu speichern. Wenn Ereignisse verarbeitet werden, werden in diesen Tabellen die Monitor-Modellinstanzdaten gespeichert. Die Dashboards verweisen dann auf diese Tabellen.

**Tipp:** In einer Network Deployment-Umgebung müssen die Datenbanken MONITOR und COGNOSCS erstellt werden, bevor Deployment Manager gestartet wird und weitere angepasste Profile erstellt werden.

**Tipp:** Wenn sich die COGNOSCS-Datenbank nicht lokal auf dem IBM Cognos BI-Server befindet, müssen Sie einen Datenbankclient auf der IBM Cognos BI-Servermaschine installieren. Details hierzu enthalten die entsprechenden Abschnitte mit datenbankspezifischen Datenbankhinweisen.

## Datenbanken erstellen

Zur Erstellung der Monitor-Datenbank und der COGNOSCS-Datenbank gibt es unterschiedliche Möglichkeiten.

- Wenn die Datenbanksoftware auf demselben Server wie IBM Business Monitor installiert ist, können Sie mit dem Profile Management Tool oder mit dem Befehl 'manageprofiles' während der Profilerstellung lokale Datenbanken erstellen.

**Anmerkung:**

- Für DB2 muss der Benutzer, der das Profil erstellt, über Berechtigungsnachweise zum Erstellen der Datenbank verfügen.
- Für Oracle oder SQL Server muss die Benutzer-ID und das Kennwort eines Datenbankadministrators für das Profile Management Tool oder den Befehl 'manageprofiles' angegeben werden, damit Datenbankobjekte in einer vorhandenen Datenbankinstanz erstellt werden können.
- Sie können mit der Profilverwaltungsfunktion Datenbankskripts generieren und dazu Konfigurationswerte benutzen, die bei der Erstellung des Profils ausgewählt wurden. Wählen Sie die Option zur Profilerstellung aus, um die Ausführung der Datenbankskripts zu verzögern. Die generierten Skripts können dann in einer späteren Phase ausgeführt werden, um die Datenbankobjekte auf dem Datenbankserver zu erstellen.
- Sie können die Datenbank manuell mithilfe von Skripts erstellen, die auf den Installationsmedien oder im IBM Business Monitor-Installationsverzeichnis 'dbscripts' enthalten sind. Die Variablen in den Skripts können manuell oder mit dem Datenbankentwurfstool (DbDesignGenerator) konfiguriert werden.

**Wichtig:** Verwenden Sie diese Option mit DB2 for z/OS.

Wenn Sie in der MONITOR-Datenbank die Tabellenbereiche für Beispieldaten umbenennen, dann müssen Sie, wenn Sie das Schema für Monitor-Modelle erstellen, die Schemaerstellungsskripts exportieren und die Tabellenbereichsnamen ändern, sodass sie mit den Namen übereinstimmen, die während der Ersterstellung der Datenbank verwendet wurden.

## Datenbankgröße

Die IBM Business Monitor-Datenbankskripts für die Monitor-Datenbank erstellen mehrere Tabellenbereiche, um Daten zu speichern. Die Tabellenbereichsnamen und die Konfiguration können abhängig von den Unternehmensstandards, den Leistungs- und den Größenanforderungen geändert werden. Für Entwicklungs- und Testinstallationen mit minimalen Datenmengen reicht 1 GB Datenbankspeicher normalerweise aus. Für Produktionsumgebungen sollten Sie die Größe der Datenbank auf der Basis der Datenmenge festlegen, die Sie überwachen wollen.

## Datenbanken schützen

Wenn die Datenbanken erstellt werden, werden dem Benutzer der Laufzeitdatenbank standardmäßig Berechtigungen zur Verwaltung von Datenbankobjekten erteilt. Dies vereinfacht die Erstellung von Datenbanken und ermöglicht dem IBM Business Monitor-Server, das Datenbankschema des Monitor-Modells automatisch bei der Implementierung und Entfernung der Modelle zu verwalten. Wenn die Datenbanken geschützt werden müssen, finden Sie weitere Informationen in den Abschnitten Monitor-Datenbankumgebung schützen und IBM Cognos BI-Sicherheit konfigurieren.

## Hinweise zur MONITOR-Datenbank für DB2

Dieser Abschnitt enthält spezielle Empfehlungen für Datenbanken unter DB2.

### Hinweise zur Globalisierung

DB2 muss mit dem Universalzeichensatz UTF-8 installiert werden. Dadurch wird sichergestellt, dass die Metadaten und Instanzdaten des Monitormodells, die landessprachliche Zeichen enthalten, in der Datenbank gespeichert werden können.

Darüber hinaus ist für IBM Cognos Business Intelligence eine UTF-8-Datenbank erforderlich. Das Script `createDatabase.sql` erstellt die Datenbank automatisch im UTF-8-Format.

Das Script `createDatabase.sql` bewirkt die Erstellung der Datenbanken mit der folgenden Standardgebietseinstellung:


```
TERRITORY EN_US
```

Um die Standardsprache zu ändern, müssen Sie die Einstellung für TERRITORY in eine unterstützte Gebietseinstellung wie in DB2 Unterstützte Gebietscodes und Codepages aufgeführt ändern. Die Gebietseinstellungen müssen den codierten Zeichensatz UTF-8 verwenden. Um das Gebiet in Französisch zu ändern, müssten Sie beispielsweise folgende Angabe verwenden:





```
TERRITORY FR_FR
```

## Hinweise zu DB2 Express Edition

DB2 Express Edition kann bis zu 4 GB an Instanzspeicherplatz verwenden. Dies gilt auch dann, wenn das System über mehr als 4 GB Hauptspeicher verfügt. Weitere Informationen zu der zu verwendenden Version von DB2 finden Sie über die zugehörigen Linkverweise.

Gegenwärtig gibt es eine bekannte Einschränkung im Installationsprogramm für DB2 Express. Dieses betrifft die Einbindung von landessprachlichen Zeichenfolgen in Eigenschaften, die vom Installationsprogramm für IBM Business Monitor übergeben werden. Die folgenden Werte, die bei der Installation an DB2 Express übergeben werden, dürfen keine landessprachlichen Zeichenfolgen enthalten: 

 Windows

-  Linux Instanzbenutzername und -kennwort: `bpminst`
-  Linux Abgeschirmter Benutzername und -kennwort: `bpmfenc`
-  Linux Benutzername für den Verwaltungsserver (DAS): `bpmadmin`
-  Windows Name des Benutzers mit Verwaltungsaufgaben: `bpmadmin`

## DB2-Kataloganforderungen

Wenn sich die DB2-Datenbank nicht lokal auf dem IBM Cognos BI-Server befindet, muss die MONITOR-Datenbank durch den DB2-Client katalogisiert werden, der mit dem IBM Cognos BI-Server installiert wurde.

**Wichtig:** Stellen Sie sicher, dass der Aliasname auf dem fernen IBM Cognos BI-Server mit dem katalogisierten Datenbanknamen der MONITOR-Datenbank identisch ist. Andernfalls schlägt die Würfelerstellung fehl, wenn ein Monitormodell implementiert wird.

Ausführliche Informationen hierzu finden Sie im Thema mit den Hinweisen zur IBM Cognos BI-Datenbank.

## Hinweise zur Sicherheit der Monitor-Datenbank

Wenn Sie das Profile Management Tool (in WebSphere Customization Toolbox) oder den Befehl `'manageprofiles'` zum Erstellen der DB2-Datenbank verwenden, versucht der Benutzer mit Verwaltungsaufgaben, der das Profil erstellt, auch die

Datenbank zu erstellen. Der Benutzer der IBM Business Monitor-Laufzeitdatenbank (@DB\_USER@), der während der Profilerstellung angegeben wurde, muss im Betriebssystem bereits vorhanden sein.

Standardmäßig erhält der Benutzer der IBM Business Monitor-Laufzeitdatenbank im Rahmen der Datenbankerstellung die Berechtigungen DBADM eines Datenbankadministrators. Dadurch kann der IBM Business Monitor-Server das Datenbankschema des Monitormodells automatisch verwalten, wenn Modelle implementiert und entfernt werden. Um die Datenbank zu sichern, können Sie sie manuell erstellen und dem Benutzer der Laufzeitdatenbank nur diejenigen Berechtigungen erteilen, die für die Laufzeitoperationen auch erforderlich sind. Näheres hierzu enthalten „Monitor-Datenbank manuell installieren“ auf Seite 67 und Monitor-Datenbankumgebung schützen.

## Hinweise zu Sperren bei DB2

Bei einer großen Anzahl von Ereignissen kann es zu Monitor-Datenbankdeadlocks für zwei oder mehrere verschiedene Transaktionen kommen, die auf dieselbe Datenbank warten. Wenn dies geschieht, schlägt eine der Transaktionen fehl und wird wiederholt.

Um Deadlocks für DB2 LUW zu verhindern, dabei jedoch die gleichzeitige Verarbeitung unter hoher Datenlast beizubehalten, geben Sie im DB2-Befehlsfenster Folgendes ein:

```
db2set DB2_SKIPINSERTED=ON  
db2set DB2_SKIPDELETED =ON
```

Wenn die Variablen DB2\_SKIPINSERTED und DB2\_SKIPDELETED der DB2-Instanzregistry auf ON eingestellt werden, treten bei mehreren Threads keine Deadlocks auf.

## Hinweise zu Health Monitor

Wenn Sie DB2 Health Monitor (Automatic Maintenance) verwenden, schließen Sie SIBOWNER bei der automatischen Statistikerfassung aus. Weitere Informationen finden Sie im entsprechenden Thema in den zugehörigen Verweisen.

## Hinweise zur Cognos-Datenbank für DB2

IBM Cognos Business Intelligence verwendet die COGNOSCS-Datenbank (IBM Cognos BI-Content-Store-Datenbank) für Spezifikationsinformationen zu Konfiguration und Berichten und die MONITOR-Datenbank für die tatsächlichen Berichtsdaten.

## Hinweise zur COGNOSCS-Datenbank für IBM Cognos BI

Der IBM Cognos BI-Service erstellt Tabellen in der IBM Cognos BI-Content-Store-Datenbank, wenn diese das erste Mal erstellt wird. Da der Datenbankbenutzer, der zum Zugriff auf die Content-Store-Datenbank angegeben wird, über die Berechtigung zum Erstellen von Tabellen in der Datenbank verfügen muss, wird empfohlen, einen neuen Datenbankbenutzer nur für die Content-Store-Datenbank zu erstellen.

Die COGNOSCS-Datenbank darf nur für IBM Business Monitor-Daten verwendet werden. Daten dürfen nicht direkt zur COGNOSCS-Datenbank hinzugefügt werden. Außerdem darf die Datenbank auch nicht mit anderen Datenbanken verwen-






det werden, um Berichte für solche Daten (in Kombination mit in IBM Business Monitor erstellten Daten oder separat) zu erstellen.

## Hinweise zur MONITOR-Datenbank für IBM Cognos BI

Wenn sich Ihre MONITOR-Datenbank nicht lokal auf dem Servern oder Cluster befindet, auf dem der IBM Cognos BI-Service implementiert ist, müssen Sie einen vollständigen Datenbankclient wie IBM Data Server Client auf dem IBM Cognos BI-Server installieren, um Würfel zu implementieren.

Die ferne Datenbank muss katalogisiert werden, bevor Sie die IBM Cognos BI-Würfelpakete während der Monitor-Modell-Implementierung veröffentlichen können. Bei dem katalogisierten Namen muss es sich um den Datenbanknamen handeln, den Sie für die MONITOR-Datenbank eingegeben haben. Andernfalls müssen Sie die Datenquelle WBMONITOR\_DB in IBM Cognos BI so ändern, dass sie auf den korrekten katalogisierten Namen verweist.

IBM Cognos BI benötigt beim Veröffentlichen von Würfelpaketen während der Modellimplementierung Zugriff auf DB2-Clientbefehle.




-  Der DB2-Client muss sich in der PATH-Angabe für den Server befinden.
-   Für den DB2-Benutzer, der den IBM Business Monitor-Server startet, müssen die richtigen Umgebungsvariablen definiert sein.

## Voraussetzung: 32-Bit-Client

Der Datenbankclient, den IBM Cognos BI verwendet, um eine Verbindung zur MONITOR-Datenbank herzustellen, muss ein 32-Bit-Client sein. Auf einem Windows-System macht DB2 ohne weitere Konfiguration sowohl 64-Bit- als auch 32-Bit-Bibliotheken verfügbar. Auf einem System mit einem anderen Betriebssystem als Windows ist für IBM Cognos BI Zugriff auf die folgenden 32-Bit-DB2-Bibliotheken erforderlich:

- Bibliotheken im Verzeichnis /lib der DB2-Serverinstallation (Beispiel: /opt/ibm/db2/V9.7/lib32)
- Bibliotheken im Verzeichnis /lib des Instanzverzeichnisses (Beispiel: /home/db2inst1/sqllib/lib32)

Wenn Sie die 64-Bit-Version von DB2 und ein anderes Betriebssystem als Windows verwenden, führen Sie die folgenden Schritte aus, um einen Pfad zu den DB2-32-Bit-Bibliotheken zu konfigurieren:

1. Klicken Sie in der Administrationskonsole auf **Server > Servertypen > WebSphere Application Server > servername**. Die Anzeige 'Konfiguration' wird angezeigt.
2. Unter **Serverinfrastruktur** erweitern Sie **Java- und Prozessverwaltung** und klicken Sie auf **Prozessdefinition**.
3. Klicken Sie unter 'Weitere Eigenschaften' auf **Umgebungseinträge**. Fügen Sie wie im Folgenden beschrieben den Pfad zu den 32-Bit-Bibliotheken hinzu:
  -  Keine Änderung erforderlich.
  -   Fügen Sie den Pfad zu den DB2-32-Bit-Serverbibliotheken der folgenden Umgebungsvariable hinzu und verwenden Sie einen Doppelpunkt (:) als Begrenzer.

Für Linux und Solaris: LD\_LIBRARY\_PATH

## Hinweise zur MONITOR-Datenbank für DB2 for z/OS

Dieser Abschnitt enthält spezielle Empfehlungen für Datenbanken unter DB2 for z/OS. Eine dedizierte Speichergruppe (STOGROUP) wird für IBM Business Monitor empfohlen. Die Speichergruppe muss erstellt werden, bevor die Monitor-Datenbank erstellt wird.

### Hinweise zur Globalisierung

DB2 for z/OS muss mit dem Universalzeichensatz UTF-8 installiert werden. Dadurch wird sichergestellt, dass die Metadaten und Instanzdaten des Monitormodells, die landessprachliche Zeichen enthalten, in der Datenbank gespeichert werden können. Die Scripts `createDatabase_Monitor.sql` und `createTablespace_Monitor.sql` erstellen die Datenbank automatisch im UTF-8-Format.

Die Tabelle `DIM_TIME` enthält eine Spalte für das Auffüllen von Dashboardberichten mit einem übersetzten Monatsnamen. Die Standorteinstellungen in z/OS werden nicht zum Erstellen der Monatsnamen verwendet. Die Datei `createTable_Monitor.sql` enthält eine SQL-Anweisung, mit der Sie die Einträge für Monatsnamen außer Kraft setzen und Ihre eigenen Monatsnamen definieren können.

### Allgemeine Datenbankhinweise

DB2 for z/OS erfordert zusätzlich zwei Pufferpools. Die folgenden 32K-Pufferpools müssen vom Datenbankadministrator erstellt werden, bevor die Datenbankskripts ausgeführt werden:

- BP32K
- TMPBP32

DB2 for z/OS erfordert eine TEMP-Datenbank zum Speichern deklarierter temporärer Tabellen.

- Erstellen Sie eine dedizierte Speichergruppe `STOGROUP`, in der die IBM Business Monitor-Daten gespeichert werden können.
- Erstellen Sie eine TEMP-Datenbank und einen TEMP-Tabellenbereich, in denen die deklarierten temporären Tabellen zur Verarbeitung von verschiebbaren Cursors gespeichert werden können. Beispiele zu diesem Thema werden unten aufgeführt.

**Für DB2 for z/OS Version 8** muss eine TEMP-Datenbank und ein TEMP-Tabellenbereich erstellt werden, falls diese noch nicht vorhanden sind. Repräsentatives Beispiel für eine TEMP-Datenbankdefinition:

```
CREATE
DATABASE TEMP AS TEMP STOGROUP SYSDEFLT;
CREATE TABLESPACE
TEMP IN TEMP
USING STOGROUP SYSDEFLT
BUFFERPOOL BP32K
SEGSIZE
32;
```

**Für DB2 for z/OS Version 9 und Version 10 in einer Umgebung ohne gemeinsame Datennutzung** ist `DSNDB07` die TEMP-Datenbank und wird während der



Datenbankinstallation erstellt. Tabellenbereiche für temporäre Tabellen werden der vorhandenen TEMP-Datenbank hinzugefügt. Repräsentatives Beispiel für einen temporären Tabellenbereich:

```
CREATE TABLESPACE WBITEMP
IN DSNDB07
USING STOGROUP SYSDEFLT
BUFFERPOOL BP32K
SEGSIZE
32;
```

**Für DB2 for z/OS Version 9 und Version 10 in einer Umgebung mit gemeinsamer Datennutzung** muss eine WORKFILE-Datenbank erstellt werden. Es kann pro Subsystem nur eine WORKFILE-Datenbank erstellt werden. Repräsentatives Beispiel für das Erstellen einer WORKFILE-Datenbank und eines temporären Tabellenbereichs:

```
CREATE DATABASE WORKTEMP AS
WORKFILE STOGROUP SYSDEFLT;
CREATE TABLESPACE WBITEMP IN WORKTEMP
USING STOGROUP SYSDEFLT
BUFFERPOOL BP32K
SEGSIZE
32;
```

Detaillierte Informationen zur Konfiguration der TEMP-Datenbank und der TEMP-Tabellenbereiche finden Sie im Information Center von DB2 for z/OS. Siehe den zugehörigen Link.

**Anmerkung:** Wenn Sie DB2 for z/OS verwenden und SPUFI zur Ausführung der Datenbankskripts verwenden möchten, übertragen Sie die Dateien mithilfe von FTP auf den z/OS-Datenbankserver. Die IBM Business Monitor-Datenbankskripts enden mit einem Zeilenvorschubzeichen. Der FTP-Server unter z/OS ordnet den Zeilenvorschub für die Datenbankskripts ordnungsgemäß einem Zeilenendezeichen zu.

DB2 for z/OS Version 8 erfordert außerdem Datenbankspeicher für Arbeitsdateien bei SQL-Anweisungen mit hohem Speicherbedarf (beispielsweise Sortiervorgänge). Hierzu muss ein Tabellenbereich zur Unterstützung der Sortiervorgänge zusätzlich zu der TEMP-Datenbank für Version 8 hinzugefügt werden. In DB2 for z/OS Version 9 und 10 werden die WORKFILE-Datenbank und die TEMP-Datenbanken kombiniert. Informationen zur Vorgehensweise und zu Größenempfehlungen beim Erstellen der Datenbanken für Arbeitsdateien finden Sie im Information Center von DB2 for z/OS.

Setzen Sie zur Verbesserung des gemeinsamen Zugriffs den Subsystemparameter RRULOCK auf YES.

Wenn der Datenübertragungsservice aktiviert werden soll, erhöhen Sie die Anzahl der Sperren pro Benutzer, NUMLKUS, auf mindestens 100.000.

## JDBC-Treiber

IBM Business Monitor verwendet den JDBC 4.0-Treiber. Standardmäßig verweist das Profile Management Tool auf die Datei db2jcc4.jar, die im Pfad application\_server-stammverzeichnis\jdbcdrivers\DB2 bereitsteht. Bei Installationen mit DB2 for z/OS wird empfohlen, die JAR-Datei db2jcc.jar des JDBC 3.0-Treibers zu verwenden, der gemeinsam mit DB2 ausgeliefert wird.

## Datenbanksubstitutionsvariablen

Für die Schemagenerierung des Monitormodells für DB2 for z/OS müssen die Variablen für den Datenbanknamen und die Speichergruppe bereitgestellt werden. Zur Minimierung der manuellen Substitution von Variablen wird die folgende Datei erstellt, wenn Sie ein Profil erstellen:

```
profil-stammverzeichnis/properties/monitor_database.properties
```

Diese Datei enthält die folgenden Eigenschaften:

```
databaseName  
db2z0SStorageGroup
```

Setzen Sie `databaseName` auf den Datenbanknamen, der im Profile Management Tool oder im Befehl **manageprofiles** zur Erstellung der Datenbank verwendet wurde. Setzen Sie `db2z0SStorageGroup` auf die DB2-Speichergruppe für die MONITOR-Datenbank. Werden die Variablennamen leer gelassen, werden die Werte für die Variablen in den Scripts zum Erstellen des Schemas für die Monitormodelle nicht ersetzt.

## Hinweise zu Cognos-Datenbanken für DB2 for z/OS

IBM Cognos Business Intelligence verwendet die COGNOSCS-Datenbank (IBM Cognos BI-Content-Store-Datenbank) für Spezifikationsinformationen zu Konfiguration und Berichten und die MONITOR-Datenbank für die tatsächlichen Berichtsdaten.

### Hinweise zu COGNOSCS-Datenbanken für IBM Cognos BI

Der IBM Cognos BI-Service erstellt Tabellen in der IBM Cognos BI-Content-Store-Datenbank, wenn diese das erste Mal erstellt wird. Da der Datenbankbenutzer, der zum Zugriff auf die Content-Store-Datenbank angegeben wird, über die Berechtigung zum Erstellen von Tabellen in der Datenbank verfügen muss, wird empfohlen, einen neuen Datenbankbenutzer nur für die Content-Store-Datenbank zu erstellen.

Die COGNOSCS-Datenbank darf nur für IBM Business Monitor-Daten verwendet werden. Daten dürfen nicht direkt zur COGNOSCS-Datenbank hinzugefügt werden. Außerdem darf die Datenbank auch nicht mit anderen Datenbanken verwendet werden, um Berichte für solche Daten (in Kombination mit in IBM Business Monitor erstellten Daten oder separat) zu erstellen.

Für DB2 for z/OS müssen Sie die Datenbank und die Tabellenbereiche manuell erstellen. Aktualisieren Sie die Tabellenerstellungsscripts, die von DB2 beim Starten verwendet werden, mit den Datenbank- und Tabellenbereichsnamen, die erstellt wurden.




### Hinweise zur MONITOR-Datenbank für IBM Cognos BI

Wenn sich Ihre MONITOR-Datenbank nicht lokal auf dem Server oder Cluster befindet, auf dem der IBM Cognos BI-Service implementiert ist, müssen Sie einen vollständigen Datenbankclient wie DB2 Connect auf dem IBM Cognos BI-Server installieren, um Würfel zu implementieren.

Die ferne Datenbank muss katalogisiert werden, bevor Sie die IBM Cognos BI-Würfelpakete während der Monitor-Modell-Implementierung veröffentlichen können. Bei dem katalogisierten Namen muss es sich um den Datenbanknamen han-

deln, den Sie für die MONITOR-Datenbank eingegeben haben. Andernfalls müssen Sie die Datenquelle WBMONITOR\_DB in IBM Cognos BI so ändern, dass sie auf den korrekten katalogisierten Namen verweist.

IBM Cognos BI benötigt beim Veröffentlichen von Würfelpaketen während der Modellimplementierung Zugriff auf DB Connect-Clientbefehle.




-  **Windows** Der DB2 Connect-Client muss sich innerhalb der PATH-Angabe für den Server befinden.
-  **Linux**  **UNIX** Für den DB2-Benutzer, der den IBM Business Monitor-Server startet, müssen die richtigen Umgebungsvariablen definiert sein.

### Voraussetzung: 32-Bit-Client

Der Datenbankclient, den IBM Cognos BI verwendet, um eine Verbindung zur MONITOR-Datenbank herzustellen, muss ein 32-Bit-Client sein. Auf einem Windows-System macht DB2 Connect ohne weitere Konfiguration sowohl 64-Bit- als auch 32-Bit-Bibliotheken verfügbar. Auf einem System mit einem anderen Betriebssystem als Windows ist für IBM Cognos BI Zugriff auf die folgenden 32-Bit-Versionen von DB2 Connect-Bibliotheken erforderlich:

- Bibliotheken im Verzeichnis /lib der DB2 Connect-Serverinstallation (Beispiel: /opt/ibm/db2/V9.7/lib32)
- Bibliotheken im Verzeichnis /lib des Instanzverzeichnisses (Beispiel: /home/db2inst1/sqllib/lib32)

Wenn Sie die 64-Bit-Version von DB2 Connect und ein anderes Betriebssystem als Windows verwenden, führen Sie die folgenden Schritte aus, um einen Pfad zu den 32-Bit-Bibliotheken von DB2 Connect zu konfigurieren:

1. Klicken Sie in der Administrationskonsole auf **Server > Servertypen > WebSphere Application Server > servername**. Die Anzeige 'Konfiguration' wird angezeigt.
2. Unter **Serverinfrastruktur** erweitern Sie **Java- und Prozessverwaltung** und klicken Sie auf **Prozessdefinition**.
3. Klicken Sie unter 'Weitere Eigenschaften' auf **Umgebungseinträge**. Fügen Sie wie im Folgenden beschrieben den Pfad zu den 32-Bit-Bibliotheken hinzu:
  -  **Windows** Keine Änderung erforderlich.
  -  **Linux**  **UNIX** Fügen Sie den Pfad zu den DB2 Connect-32-Bit-Serverbibliotheken der folgenden Umgebungsvariable hinzu und verwenden Sie einen Doppelpunkt (:) als Begrenzer.  
Für Linux und Solaris: LD\_LIBRARY\_PATH  
Für AIX: LIBPATH

## Hinweise zur MONITOR-Datenbank für Oracle

Dieser Abschnitt enthält spezielle Empfehlungen für Datenbanken unter Oracle.

### Hinweise zur Globalisierung

Oracle muss mit dem Universalzeichensatz UTF-8 (AL32UTF8) und nicht mit dem Standard-Datenbankzeichensatz (WE8ISO8859P1 - ISO 8859-1 West European) installiert werden. Dadurch wird sichergestellt, dass die Metadaten und Instanzdaten des Monitormodells, die landessprachliche Zeichen enthalten, in der Datenbank gespeichert werden können. Darüber hinaus ist für IBM Cognos BI eine UTF-8-Datenbank erforderlich.

Oracle verwaltet die Sprach- und Ländereinstellungen mit den folgenden zwei Datenbankparametern:

NLS\_LANGUAGE  
NLS\_TERRITORY

Um die Standardsprache für die Datenbanken zu ändern, müssen Sie den Wert für den Parameter NLS\_LANGUAGE in eine für Oracle unterstützte Sprache ändern. Die Gebietseinstellungen definieren, welche Datumsformatierung, Währung usw. standardmäßig verwendet wird. Geben Sie einen Wert für den Parameter NLS\_TERRITORY an, um entsprechende Änderungen bei der Oracle-Instanz zu erzielen.

Die Tabelle DIM\_TIME enthält eine Spalte für das Auffüllen von Dashboardberichten, die Zeitdimensionen enthalten, mit einem übersetzten Monatsnamen. Standardmäßig wird der Code für die Ländereinstellung für die Einstellung NLS\_LANGUAGE zum Auffüllen der Einträge der Tabelle DIM\_TIME verwendet. Wenn Sie die Standardsprache ändern möchten, müssen Sie die Angabe für NLS\_LANGUAGE für die Oracle-Instanz oder für die aktuelle Sitzung ändern, bevor Sie das Script createTables.sql ausführen. Die Datei createTables.sql enthält auch eine SQL-Anweisung, mit der Sie die Einträge für Monatsnamen außer Kraft setzen und Ihre eigenen Monatsnamen definieren können.

## Hinweise zur Monitor-Sicherheit

Wenn Sie das Profile Management Tool (in WebSphere Customization Toolbox) oder den Befehl 'manageprofiles' zum Erstellen der Oracle-Datenbankobjekte verwenden, erstellt der Datenbankbenutzer mit Verwaltungsaufgaben (Administrator), der bei der Profilerstellung angegeben wurde, auch die Datenbankobjekte und ein MONITOR-Schema. Unter Oracle stellt ein Schema sowohl eine Gruppe von Datenbankobjekten als auch eine Benutzer-ID dar, die sich bei der Datenbank anmelden kann.

Standardmäßig ist der Eigner des MONITOR-Schemas auch der Benutzer der Laufzeitdatenbank und erhält die Berechtigungen zum Erstellen anderer Schemas und Datenbankobjekte im Rahmen der Datenbankerstellung. Dadurch kann der IBM Business Monitor-Server das Datenbankschema des Monitormodells automatisch verwalten, wenn Modelle implementiert und entfernt werden. Um die Datenbank zu sichern, können Sie sie manuell erstellen. Der Eigner des MONITOR-Schemas oder ein anderer Benutzer kann als Benutzer der IBM Business Monitor-Laufzeitdatenbank verwendet werden. In einer gesicherten Umgebung können Sie dem Benutzer der MONITOR-Laufzeitdatenbank nur die Berechtigungen erteilen, die zur Ausführung der Laufzeitoperationen erforderlich sind. Weitere Informationen finden Sie in den Abschnitten "Datenbank manuell installieren" und "Monitor-Datenbankumgebung schützen" in den zugehörigen Links.

## JDBC-Treiber

Die JDBC-Unterstützung wird von den Oracle JDBC-Treibern für JVM 1.6 zur Verfügung gestellt. Die JDBC-Treiberdatei ojdbc6.jar enthält den von Oracle unterstützten JDBC-Treiber zur Verwendung mit WebSphere Application Server Version 7. Die Datei ojdbc6.jar kann sowohl für Oracle 10g als auch für Oracle 11g verwendet werden. Weitere Informationen zu Mindesteinstellungen für Oracle erhalten Sie über den zugehörigen Link.

Standardmäßig verweist das Profile Management Tool auf die Datei ojdbc6.jar, die im Pfad application\_server-stammverzeichnis\jdbcdrivers\Oracle bereit-

steht. Alternativ hierzu können Sie eine weitere JDBC-Treiberdatei Oracle `ojdbc6.jar` herunterladen und beim Ausführen des Profile Management Tool oder beim Ausführen des Befehls **manageprofiles** auf diese verweisen.

## XA-Wiederherstellung

Sie müssen besondere Grants erteilen, damit die XA-Wiederherstellung von Oracle ordnungsgemäß ausgeführt werden kann. Führen Sie als Benutzer SYS die folgenden Befehle aus:

```
grant select on pending_trans$ to <benutzer>;
grant select on dba_2pc_pending to <benutzer>;
grant select on dba_pending_transactions to <benutzer>;
grant execute on dbms_system to <benutzer>;
```

Dabei ist *<benutzer>* der Benutzername für die Monitor-Datenbank, die während der Profilerstellung konfiguriert wird.

## Generierte Sichten

Die Leistung für das Laden von Dashboardseiten kann sinken, wenn Sie große Volumen an Überwachungsdaten in Ihrer Datenbank akkumulieren. Wenn sich über 10 Millionen Monitoring-Kontextinstanzen angesammelt haben, kann es sinnvoll sein, die Option Ihres Datenbankanbieters zur Vorabberechnung der Daten zu aktivieren.

Bei Verwendung von DB2 können Sie MQTs (Materialized Query Tables) zur Leistungsverbesserung verwenden, wie dies im Abschnitt „Aktualisierung der Würfelübersichtstabelle verwalten“ beschrieben ist. Bei Oracle können Sie generierte Sichten (Materialized Views) für denselben verwenden.

Wie eine MQT in DB2 kann eine generierte Sicht die Werte von KPIs (wesentliche Leistungsindikatoren) und von IBM Cognos BI-Cube-Kennzahlen (Würfelkennzahlen) in Oracle vorab berechnen. Wenn das Dashboard einen Wert anfordert, wird kein Aggregationswert, zum Beispiel ein Durchschnittswert, der für alle Monitoring-Kontextinstanzen erst berechnet wird, sondern der vorab berechnete Wert nahezu unverzüglich zurückgegeben.

Für die Definition einer generierten Sicht (Materialized View) gibt der Oracle-Datenbankadministrator (DBA) die folgenden Einstellungen an:

### ON COMMIT

Aktualisiert (REFRESH) die generierte Sicht automatisch, wenn eine Transaktion, die Daten in der Tabelle ändern, festgeschrieben wird (d. h. wenn der Datenverschiebungsservice ausgeführt wird).

**FAST** Führt eine inkrementelle Aktualisierung von Daten während der REFRESH-Operation aus.

Ein Beispielscript, das eine generierte Sicht mit FAST und ON COMMIT für das Präsentationsbeispiel (Better Lender) definiert, finden Sie im folgenden Verzeichnis: `application_server-stammverzeichnis\installableApps.wbm\showcase\OracleMaterializedViews_Sample.`

## Hinweise zur Cognos-Datenbank für Oracle

IBM Cognos Business Intelligence verwendet die COGNOSCS-Datenbank (IBM Cognos BI-Content-Store-Datenbank) für Spezifikationsinformationen zu Konfiguration und Berichten und die MONITOR-Datenbank für die tatsächlichen Berichtsdaten.

### Hinweise zur COGNOSCS-Datenbank für IBM Cognos BI

Der IBM Cognos BI-Service erstellt Tabellen in der IBM Cognos BI-Content-Store-Datenbank, wenn diese das erste Mal erstellt wird. Der Datenbankbenutzer, der für den Zugriff auf die IBM Cognos BI-Content-Store-Datenbank angegeben wurde, muss über uneingeschränkten Zugriff auf Oracle verfügen, um Tabellen, Sichten, Sequenzen, Auslöser und weitere Elemente zu erstellen. In IBM Cognos BI ist es nicht möglich, einen separaten Schemanamen anzugeben; die IBM Cognos BI-Objekte werden im Standardschema und Standardtabellenbereich des Datenbankbenutzers erstellt. Es wird empfohlen, einen neuen Datenbankbenutzer zur ausschließlichen Verwendung in der Content-Store-Datenbank zu erstellen.

**Wichtig:** Verwenden Sie für diesen Zweck nicht den SYSTEM-Benutzer, da die IBM Cognos BI-Datenbankobjekte nicht im Systembereich erstellt werden sollen.

Die COGNOSCS-Datenbank darf nur für IBM Business Monitor-Daten verwendet werden. Daten dürfen nicht direkt zur COGNOSCS-Datenbank hinzugefügt werden. Außerdem darf die Datenbank auch nicht mit anderen Datenbanken verwendet werden, um Berichte für solche Daten (in Kombination mit in IBM Business Monitor erstellten Daten oder separat) zu erstellen.

### Hinweise zur MONITOR-Datenbank für IBM Cognos BI

Wenn sich Ihre MONITOR-Datenbank nicht lokal auf dem Server oder Cluster befindet, auf dem der IBM Cognos Business Intelligence-Service implementiert ist, müssen Sie einen vollständigen Datenbankclient oder den Oracle Instant Client auf dem IBM Cognos BI-Server installieren, um Würfel zu implementieren.

Die Oracle-Instanz für IBM Cognos BI muss über einen TNSNAMES-Eintrag im Oracle-Client auf dem IBM Cognos BI-Server angesprochen werden können. Der Eintrag in TNSNAMES muss denselben Namen als Datenbankinstanznamen verwenden wie den Namen, den Sie während der Profilerstellung für die MONITOR-Datenbank eingegeben haben (zum Beispiel ORCL). Andernfalls müssen Sie die Datenquelle WBMONITOR\_DB in IBM Cognos BI so ändern, dass sie auf den korrekten TNSNAMES-Eintrag verweist.

Wenn Sie Oracle Instant Client verwenden, muss sich der Pfad zum Client im Systempfad befinden. Außerdem muss eine Datei TNSNAMES.ORA mit einem Eintrag für den Oracle-Datenbankserver eingebunden werden und die Umgebungsvariable TNS\_ADMIN muss auf das Verzeichnis verweisen, das die Datei TNSNAMES.ORA enthält.

**Wichtig:** Installieren Sie das SQLPlus-Befehlsdienstprogramm mit Oracle Instant Client für eine spätere Fehlerbehebung.

Das folgende Beispiel zeigt den Inhalt einer gültigen Datei TNSNAMES.ORA. (Bei der in Großbuchstaben geschriebenen Zeichenfolge ORCL handelt es sich um den Aliasnamen für die Datenbankverbindung.)






```

ORCL =
(DESCRIPTION =
(AADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.1)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = orcl)
)
)

```

IBM Cognos BI benötigt beim Veröffentlichen von Würfelpaketen während der Modellimplementierung Zugriff auf Oracle-Clientbefehle.

-  Der Oracle-Client muss sich innerhalb der PATH-Angabe für den Server befinden.
-   Der Benutzer, der den IBM Business Monitor-Server startet, muss über das Profil eines Oracle-Benutzers verfügen.

## Oracle Instant Client

Zur Verwendung von Oracle Instant Client müssen Sie die folgenden Bibliotheken herunterladen und installieren:




- Instant Client Package - Basic Instant Client Package
- SQL\*Plus (hilfreich für die Fehlerbehebung bei der Verbindung)

Fügen Sie dem Serverpfad das Installationsverzeichnis hinzu und erstellen Sie eine Datei TNSNAMES.ORA wie im vorherigen Abschnitt beschrieben. Fügen Sie eine Umgebungsvariable TNS\_ADMIN hinzu und geben Sie den Pfad zu dem Verzeichnis an, das die Datei TNSNAMES.ORA enthält.

## Voraussetzung: 32-Bit-Client

Für die IBM Cognos BI-Würfelimplementierung muss ein Oracle-32-Bit-Client installiert sein. Ist Oracle auf einem separaten Server installiert, wird der Oracle Instant Client mit 32 Bit empfohlen. Ist Oracle auf demselben Server wie IBM Cognos BI und die 64-Bit-Version von Oracle installiert, muss der Oracle Instant Client mit 32 Bit ebenfalls installiert sein.

Wenn Sie die 64-Bit-Version von Oracle verwenden, führen Sie die folgenden Schritte aus, um einen Pfad zu den Oracle-32-Bit-Bibliotheken zu konfigurieren:

1. Klicken Sie in der Administrationskonsole auf **Server > Servertypen > WebSphere Application Server > servername**. Die Anzeige 'Konfiguration' wird angezeigt.
2. Unter **Serverinfrastruktur** erweitern Sie **Java- und Prozessverwaltung** und klicken Sie auf **Prozessdefinition**.
3. Klicken Sie unter 'Weitere Eigenschaften' auf **Umgebungseinträge**. Fügen Sie wie im Folgenden beschrieben den Pfad zu dem Oracle Instant Client hinzu:
  -  Fügen Sie der Umgebungsvariablen PATH den Pfad zu dem Oracle Instant Client mit 32 Bit hinzu und verwenden Sie ein Semikolon (;) als Begrenzer.
  -   Fügen Sie der folgenden Umgebungsvariablen den Pfad zu dem Oracle Instant Client mit 32 Bit hinzu und verwenden Sie einen Doppelpunkt (:) als Begrenzer.

Für Linux und Solaris: LD\_LIBRARY\_PATH

Für AIX: LIBPATH

## Hinweise zur MONITOR-Datenbank für Microsoft SQL Server

Dieser Abschnitt enthält spezielle Empfehlungen für Datenbanken unter Microsoft SQL Server.

**Wichtig:** Bei der Installation von SQL Server müssen Sie als Authentifizierungsmodus den gemischten Modus (Windows-Authentifizierung oder SQL Server-Authentifizierung) auswählen.

**Wichtig:** Zur Verwendung von SQL Server mit IBM Business Monitor müssen Sie SQL Server für XA-Transaktionen konfigurieren. SQL Server ist nicht für XA-Transaktionen vorkonfiguriert. Die XA-Unterstützung wird im Rahmen der Microsoft-JDBC-Treiberdistribution bereitgestellt und enthält die DLL (Dynamic Link Library) 'sqljdbc\_xa.dll' sowie das Installationsscript 'xa\_install.sql'. Da XA-Transaktionen standardmäßig nicht aktiviert sind, müssen Sie die Konfiguration in Microsoft Windows Distributed Transaction Coordinator (MSDTC) ändern. Anweisungen zum Aktivieren der XA-Unterstützung für SQL Server enthält der Abschnitt 'Grundlegendes zu XA-Transaktionen' in der Onlinedokumentation zu Microsoft SQL Server.

Wenn Sie das Profile Management Tool (in WebSphere Customization Toolbox) oder den Befehl 'manageprofiles' zum Erstellen der SQL Server-Datenbank verwenden, erstellt der Datenbankbenutzer mit Verwaltungsaufgaben, der bei der Profilerstellung angegeben wurde, auch die Datenbank. Der Benutzer der IBM Business Monitor-Laufzeitdatenbank (@DB\_USER@), der während der Profilerstellung angegeben wurde, muss bereits als Anmelde- und Datenbankbenutzer von SQL Server vorhanden sein. Sie können den folgenden Befehl verwenden, um den Benutzer für die Datenbankanmeldung und den Datenbankbenutzer zu erstellen:

```
CREATE LOGIN @DB_BENUTZER@ WITH PASSWORD = '@DB_KENNWORT@', DEFAULT_DATABASE=@DB_NAME@
CREATE USER @DB_BENUTZER@ FOR LOGIN @DB_BENUTZER@
```

Hierbei steht DB\_BENUTZER für den Benutzer der IBM Business Monitor-Laufzeitdatenbank, DB\_KENNWORT für das Kennwort der Laufzeitdatenbank und DB\_NAME für den Namen der IBM Business Monitor-Datenbank.

Standardmäßig erhält der Benutzer der IBM Business Monitor-Laufzeitdatenbank im Rahmen der Datenbankeinstellung die Berechtigungen von 'db\_owner'. Dadurch kann der IBM Business Monitor-Server das Datenbankschema des Monitormodells automatisch verwalten, wenn Modelle implementiert und entfernt werden. Um die Datenbank zu sichern, können Sie sie manuell erstellen und dem Benutzer der Laufzeitdatenbank nur diejenigen Berechtigungen erteilen, die für die Laufzeitoperationen auch erforderlich sind. Weitere Informationen finden Sie in den Abschnitten "Datenbank manuell installieren" und "Monitor-Datenbankumgebung schützen" in den zugehörigen Links.

Die SQL Server-JDBC-Treiber für JVM 1.6 bieten JDBC-Unterstützung. IBM Business Monitor verwendet die Datei sqljdbc4.jar des Microsoft JDBC 2.0-Treibers. Standardmäßig verweist das Profile Management Tool auf die Datei sqljdbc4.jar, die im Pfad application\_server-stammverzeichnis\jdbcdrivers\SQLServer bereitsteht. Alternativ hierzu können Sie eine weitere JDBC-Treiberdatei sqljdbc4.jar herunterladen und beim Ausführen des Profile Management Tool oder beim Ausführen des Befehls **manageprofiles** auf diese verweisen. Informationen zu den erforderlichen Mindesteinstellungen für SQL Server erhalten Sie über den zugehörigen Link.



## Hinweise zur Globalisierung

SQL Server verwaltet bei der Erstellung der Datenbank die Ländereinstellungen mit der Option COLLATE. Die Erstellungsanweisung für die Datenbanken MONITOR und COGNOSCS enthält die folgende Option:

```
COLLATE SQL_Latin1_General_CP1_CS_AS
```

Um die Ländereinstellungen zu ändern, müssen Sie den Parameter COLLATE für die Sortierung in eine für die gewünschte Sprache unterstützte Sortierung ändern. Um die Sortierung in Französisch zu ändern, müssten Sie beispielsweise folgende Angabe verwenden:

```
COLLATE French_100_CS_AS
```

SQL Server verwaltet die Standardsprache auf der Grundlage des Anmeldebenutzers. Um die Standardsprache zu ändern, müssen Sie in der Datei createDatabase.sql die Option DEFAULT\_LANGUAGE zu der Anweisung für die Anmeldeerstellung (CREATE LOGIN) mit einer anderen Standardsprache hinzufügen. Um die Anmeldung mit Französisch als Standardsprache zu erstellen, müssten Sie beispielsweise folgende Angabe verwenden:

```
IF NOT EXISTS (SELECT * FROM syslogins WHERE NAME = '@DB_USER@') CREATE LOGIN @DB_USER@ WITH PASS
```

Die Tabelle DIM\_TIME enthält eine Spalte für das Auffüllen von Dashboardberichten, die Zeitdimensionen enthalten, mit einem übersetzten Monatsnamen. Standardmäßig wird der Code für die Ländereinstellung für die Einstellung DEFAULT\_LANGUAGE zum Auffüllen der Einträge der Tabelle DIM\_TIME verwendet. Wenn Sie die Standardsprache ändern möchten, müssen Sie die Angabe für DEFAULT\_LANGUAGE für den Datenbankbenutzer ändern, bevor Sie das Script createTables.sql ausführen. Die Datei createTables.sql enthält auch eine SQL-Anweisung, mit der Sie die Einträge für Monatsnamen außer Kraft setzen und Ihre eigenen Monatsnamen definieren können.

## Hinweise zur Cognos-Datenbank für Microsoft SQL Server

IBM Cognos Business Intelligence verwendet die COGNOSCS-Datenbank (IBM Cognos BI-Content-Store-Datenbank) für Spezifikationsinformationen zu Konfiguration und Berichten und die MONITOR-Datenbank für die tatsächlichen Berichtsdaten.

**Wichtig:** Die IBM Cognos BI-Datenbank benötigt eine Sortierung, bei der die Groß-/Kleinschreibung nicht beachtet wird, während die IBM Business Monitor-Datenbank eine Sortierung erfordert, bei der die Groß-/Kleinschreibung berücksichtigt wird. Wenn die standardmäßige Sortierung für die IBM Cognos BI-Datenbank geändert wird, so darf bei dieser Sortierung die Groß-/Kleinschreibung nicht beachtet werden.

## Hinweise zur COGNOSCS-Datenbank für IBM Cognos BI

Der IBM Cognos BI-Service erstellt Tabellen in der IBM Cognos BI-Content-Store-Datenbank, wenn diese das erste Mal erstellt wird. Da der Datenbankbenutzer, der zum Zugriff auf die Content-Store-Datenbank angegeben wird, über die Berechtigung zum Erstellen von Tabellen in der Datenbank verfügen muss, wird empfohlen, einen neuen Datenbankbenutzer nur für die Content-Store-Datenbank zu erstellen.

Die COGNOSCS-Datenbank darf nur für IBM Business Monitor-Daten verwendet werden. Daten dürfen nicht direkt zur COGNOSCS-Datenbank hinzugefügt wer-

den. Außerdem darf die Datenbank auch nicht mit anderen Datenbanken verwendet werden, um Berichte für solche Daten (in Kombination mit in IBM Business Monitor erstellten Daten oder separat) zu erstellen.

## Hinweise zur MONITOR-Datenbank für IBM Cognos BI

Wenn sich Ihre MONITOR-Datenbank nicht lokal auf dem Server oder Cluster befindet, auf dem der IBM Cognos Business Intelligence-Service implementiert ist, müssen Sie einen vollständigen Microsoft SQL Server-Datenbankclient auf dem IBM Cognos BI-Server installieren, um Würfel zu implementieren.

Microsoft bietet einen SQL Server Native Client, der anstelle der vollständigen SQL Server-Clientinstallation verwendet werden kann. Diese Mindestinstallation enthält alle erforderlichen nativen Treiber. Parallel zum nativen Client sollten Sie auch die SQL Server-Befehlszeilendienstprogramme herunterladen und installieren. Beide Produkte können über die Seite Microsoft SQL Server 2008 Feature Pack, August 2008 bezogen werden.

IBM Cognos BI benötigt beim Veröffentlichen von Würfelpaketen während der Modellimplementierung Zugriff auf SQL Server-Clientbefehle. Der SQL Server-Client muss sich innerhalb der PATH-Angabe für den Server befinden.

---

## Hinweise zur Benutzerregistry

In der Benutzerregistry werden Informationen gespeichert, die für die Authentifizierung von Benutzern über die Basisauthentifizierung verwendet werden. Die Auswahl der Benutzerregistry ist von wesentlicher Bedeutung bei der Planung einer Umgebung. Sie müssen WebSphere Application Server für die Verwendung der Benutzerregistry in der jeweiligen Umgebung konfigurieren.

In der Benutzerregistry werden Informationen gespeichert, die für die Authentifizierung von Benutzern verwendet werden, die Zugriff auf IBM Business Monitor anfordern. Sie können eine Reihe verschiedener Benutzerregistrytypen als eingebundene Repositorys konfigurieren. In den meisten Implementierungen in Produktionsumgebungen wird ein LDAP-Server (Lightweight Directory Access Protocol) verwendet. Für kleine Implementierungen auf einem einzigen Server können Sie eine dateibasierte Benutzerregistry verwenden.

Sie können aus folgenden Möglichkeiten als Repository für Ihr Benutzeraccount auswählen:

- Eingebundene Repositorys
- Lokales Betriebssystem
- Eigenständige LDAP-Registry
- Eigenständige angepasste Registry

**Anmerkung:** Bei differenzierter (detaillierter) Sicherheit werden eingebundene (föderierte) Repositorys (dateibasiert), eingebundene (föderierte) Repositorys (LDAP) und eigenständige LDAP-Registries als Benutzerregistries unterstützt.

---

## Hinweise für Benutzer ohne Verwaltungsaufgaben



Wenn Sie die Installation von IBM Business Monitor als Benutzer ohne Rootberechtigung bzw. Benutzer ohne Verwaltungsaufgaben vornehmen und während der Installation ein Testprofil installieren möchten, muss der DB2-Server installiert sein, bevor Sie mit der Installation beginnen. Halten Sie alle Einzelinformationen zur Datenbank bereit, damit Sie sie während der Installation eingeben können.

Die in diesem Abschnitt erläuterten Hinweise gelten für alle Installationsszenarien, bei denen Sie sich für eine **typische Installation** entscheiden. Die Erstellung von Profilen erfolgt automatisch, wenn Sie die Installation unter Verwendung der Installationsoption für eine **typische Installation** (Standardinstallation) vornehmen.

Bei einer Installation als Benutzer ohne Verwaltungsaufgaben haben Sie die folgenden Möglichkeiten: 

- Installieren Sie einen separaten DB2-Server, bevor Sie die eigentliche Produktinstallation vornehmen. Informationen zur Installation von DB2 als Benutzer ohne Administrator- oder Rootberechtigung finden Sie in folgenden Abschnitten:



-  Übersicht zur Installation ohne Rootberechtigung (Linux und UNIX)
-  Erforderliche Benutzeraccounts zur Installation von DB2-Serverprodukten (Windows)
- Melden Sie sich als Administrator an und installieren Sie mithilfe des Installationsprogramms für das Produkt nur den DB2-Server. Erteilen Sie dem Benutzer ohne Verwaltungsaufgaben eine spezielle Berechtigung. Melden Sie sich dann als dieser Benutzer ohne Verwaltungsaufgaben an und installieren Sie das Produkt unter Verwendung des installierten DB2-Servers.

Anstatt ein Testprofil zu erstellen, können Sie alternativ nach der Installation ein Profil erstellen. Führen Sie die folgenden Schritte aus:

1. Installieren Sie das Produkt, ohne ein Profil zu erstellen. Wenn Sie die Installation als Benutzer ohne Verwaltungsaufgaben ausführen, müssen Sie auf der Seite für die Installationspakete das Kontrollkästchen für DB2 Express abwählen. Unter Windows müssen Sie, sofern die Option zum Installieren von IBM Cognos Business Intelligence angeboten wird, dieses Kontrollkästchen ebenfalls abwählen.
2. Erweitern Sie auf der Seite für Features die Server und stellen Sie sicher, dass keine Testprofile ausgewählt sind.
3. Erstellen Sie mit dem Profile Management Tool ein eigenständiges Profil oder die Deployment Manager-Profile und die benutzerdefinierten Profile. Wenn keine Datenbank installiert ist, verwenden Sie für alle Schritte den Pfad **Erweitert**. Verwenden Sie nicht den Pfad für **Typisch**. Wählen Sie die Option für die Ausführung der Datenbankskripts während der Profilerstellung zu einem späteren Zeitpunkt aus.
4. Falls die Datenbanken nicht im Voraus erstellt wurden, lassen Sie die Erstellung der Datenbanken und Tabellen nach der Profilerstellung oder -erweiterung vom Datenbankadministrator vornehmen.
5. Weitere Vorgehensweise bei einer Netzimplementierung:
  - a. Binden Sie die angepassten (benutzerdefinierten) Profil in den Deployment Manager ein.

- b. Erstellen Sie die erforderliche Implementierungsumgebung mit der Administrationskonsole.

---

## Hinweise zur Topologie

In IBM Business Monitor können Sie unter verschiedenen Konfigurationspfaden für Ihre Implementierungsumgebung auswählen.

Eine zellenübergreifende Umgebung ist eine Umgebung, in der IBM Business Monitor Ereignisse von einem Server empfängt, der sich in einer anderen Zelle als der IBM Business Monitor-Server befindet. Eine zellenübergreifende Umgebung kann eine Network Deployment- oder eine Einzelservertopologie enthalten. In beiden Fällen müssen Sie einige Schritte ausführen, um die Kommunikation zwischen dem CEI-Server und dem IBM Business Monitor-Server zu ermöglichen. Informationen zur Aktivierung der zellenübergreifenden Kommunikation finden Sie im Abschnitt 'Empfang von Ereignissen konfigurieren'. Ein Beispiel für eine zellenübergreifende Topologie enthält das Szenario 'Ereignisse von einem SAP-EIS ohne Mediation überwachen'.

## Hinweise für eine Einzelservertopologie

Bei Verwendung der Einzelservertopologie werden IBM Business Monitor und alle erforderlichen Komponenten auf demselben physischen Server installiert.

Gehen Sie wie folgt vor, um den IBM Business Monitor-Server und alle erforderlichen Komponenten auf demselben Server zu installieren:

1. Führen Sie die Schritte zur Installationsvorbereitung im Abschnitt Kapitel 3, „Installation vorbereiten“, auf Seite 35 aus.
2. Installieren Sie IBM Business Monitor, wie im Abschnitt Kapitel 4, „IBM Business Monitor-Software installieren“, auf Seite 41 beschrieben. Bei der Installation des Produkts haben Sie die Möglichkeit, ein Entwicklungsprofil zu erstellen, das eine -Testumgebung bereitstellt, aber nicht in einer Produktionsumgebung verwendet werden kann.
3. Wenn Sie kein Entwicklungsprofil erstellt haben, erstellen Sie mit dem Profile Management Tool oder dem Befehl 'manageprofiles' ein eigenständiges Profil, wie im Abschnitt Kapitel 6, „Profile erstellen und erweitern“, auf Seite 87 beschrieben.

Alle erforderlichen IBM Business Monitor-Komponenten werden automatisch installiert und konfiguriert.

Optional können Sie den Status der Komponenten überprüfen und über den Konfigurationsassistenten in der Administrationskonsole Aktualisierungen durchführen.

## Hinweise für eine Network Deployment-Topologie unter Verwendung von Implementierungsumgebungsmustern

Die Netzimplementierung (Network Deployment) in IBM Business Monitor baut auf Netzimplementierungsfunktionen auf, die in WebSphere Application Server Network Deployment implementiert sind. Wenn Sie eines der verfügbaren Implementierungsumgebungsmuster auswählen, hilft Ihnen der Implementierungsumgebungsassistent bei der Konfiguration der Cluster, Server und Komponenten, die Sie benötigen.

Wenn Sie mit der Netzimplementierung in WebSphere Application Server Network Deployment vertraut sind, werden Sie die Konzepte wiedererkennen. Es sind zwei

Muster für IBM Business Monitor, verfügbar: das Ein-Cluster-Muster und das Vier-Cluster-Muster für fernes Messaging, Fernunterstützung und Webanwendungen.

Gehen Sie wie folgt vor, um den IBM Business Monitor-Server und alle erforderlichen Komponenten in der Ein-Cluster- oder Vier-Cluster-Implementierungsumgebung zu installieren:

1. Führen Sie die Schritte zur Installationsvorbereitung im Abschnitt Kapitel 3, „Installation vorbereiten“, auf Seite 35 aus.
2. Installieren Sie IBM Business Monitor, wie im Abschnitt Kapitel 4, „IBM Business Monitor-Software installieren“, auf Seite 41 beschrieben. Erstellen Sie kein Entwicklungsprofil.
3. Erstellen Sie mit dem Profile Management Tool oder dem Befehl `manageprofiles` ein Deployment Manager-Profil, wie im Abschnitt Kapitel 6, „Profile erstellen und erweitern“, auf Seite 87 beschrieben.
4. Falls Sie bei der Profilerstellung nicht auch gleich die Monitor-Datenbank erstellt haben, führen Sie die Scripts zum Erstellen der Datenbank aus. Gehen Sie dazu nach den Anweisungen im Abschnitt Kapitel 5, „Datenbanken erstellen“, auf Seite 59 vor.
5. Starten Sie den Deployment Manager.
6. Erstellen Sie angepasste Knoten, die in die Deployment Manager-Zelle eingebunden werden. Führen Sie dazu die Schritte im Abschnitt Kapitel 6, „Profile erstellen und erweitern“, auf Seite 87 aus.
7. Normalerweise können Sie bei der Erstellung der Implementierungsumgebung zwischen dem Ein-Cluster-Muster und dem Vier-Cluster-Muster (Fernes Messaging, Fernunterstützung und Webanwendungen) auswählen. Führen Sie die Schritte im Abschnitt „Implementierungsumgebung mit einem Muster erstellen“ auf Seite 121 aus.
8. Konfigurieren Sie die zusätzlichen Komponenten wie z. B. Business Space und IBM Cognos BI und befolgen Sie dabei die Anweisungen in Kapitel 10, „IBM Business Monitor-Komponenten konfigurieren“, auf Seite 167.

Die Cluster werden erstellt und alle erforderlichen IBM Business Monitor-Komponenten automatisch installiert und konfiguriert.

Optional können Sie den Status der Komponenten überprüfen und über den Konfigurationsassistenten in der Administrationskonsole Aktualisierungen durchführen.

## Hinweise für angepasste Network Deployment-Topologie

Statt mit dem Implementierungsumgebungsassistenten eine Ein-Cluster- oder Vier-Cluster-Topologie für Network Deployment (ND) zu erstellen, können Sie mit dem Konfigurationsassistenten oder dem Befehl `wsadmin` eine Topologie nach eigenen Vorstellungen erstellen.

Gehen Sie wie folgt vor, um den IBM Business Monitor-Server und alle erforderlichen Komponenten in einer angepassten Network Deployment-Topologie zu installieren:

1. Führen Sie die Schritte zur Installationsvorbereitung im Abschnitt Kapitel 3, „Installation vorbereiten“, auf Seite 35 aus.
2. Installieren Sie IBM Business Monitor, wie im Abschnitt Kapitel 4, „IBM Business Monitor-Software installieren“, auf Seite 41 beschrieben. Erstellen Sie kein Entwicklungsprofil.

3. Erstellen Sie mit dem Profile Management Tool oder dem Befehl `manageprofiles` ein Deployment Manager-Profil, wie im Abschnitt Kapitel 6, „Profile erstellen und erweitern“, auf Seite 87 beschrieben.
4. Falls Sie bei der Profilerstellung nicht auch gleich die Monitor-Datenbank erstellt haben, führen Sie die Scripts zum Erstellen der Datenbank aus. Gehen Sie dazu nach den Anweisungen im Abschnitt Kapitel 5, „Datenbanken erstellen“, auf Seite 59 vor.
5. Starten Sie den Deployment Manager.
6. Erstellen Sie angepasste Knoten, die in die Deployment Manager-Zelle eingebunden werden. Führen Sie dazu die Schritte im Abschnitt Kapitel 6, „Profile erstellen und erweitern“, auf Seite 87 aus.
7. Erstellen Sie die Cluster über die Administrationskonsole, wie im Abschnitt „IBM Business Monitor-Cluster erstellen“ auf Seite 139 beschrieben.
8. Konfigurieren Sie die erforderlichen CEI-Ereignisservices (Common Event Infrastructure), wie im Abschnitt „CEI-Ereignisservices konfigurieren“ auf Seite 142 beschrieben.
9. Konfigurieren Sie mit dem Konfigurationsassistenten oder dem Befehl `wsadmin` die Umgebung und befolgen Sie dabei die Anweisungen in „Umgebung mit dem Konfigurationsassistenten konfigurieren“ auf Seite 143 bzw. „Umgebung mithilfe von `wsadmin`-Befehlen konfigurieren“ auf Seite 150. Für die erforderlichen gemeinsam genutzten Komponenten müssen Sie jedoch die im Abschnitt „Umgebung manuell konfigurieren“ auf Seite 152 beschriebenen Schritte zur manuellen Konfiguration ausführen.
10. Konfigurieren Sie die zusätzlichen Komponenten wie z. B. Business Space und IBM Cognos BI und befolgen Sie dabei die Anweisungen in Kapitel 10, „IBM Business Monitor-Komponenten konfigurieren“, auf Seite 167.

## Hinweise für IBM Business Process Manager in einer Umgebung mit Vier-Cluster-Topologie

Sie können eine Vier-Cluster-Topologie mit IBM Business Process Manager konfigurieren, um eine kombinierte Implementierungsumgebung mit IBM® Business Process Manager und IBM Business Monitor nach dem (aus vier Clustern bestehendem) Muster 'Fernes Messaging, Fernunterstützung und Webanwendungen' zu erstellen. Da eine IBM Business Monitor-Implementierungsumgebung alle Anwendungen in der Zelle überwachen kann, sollten Sie nur eine IBM Business Monitor-Implementierungsumgebung in einer Zelle erstellen. Die Vier-Cluster-Topologie kombiniert IBM Business Monitor-Cluster und Cluster für die IBM Business Process Manager-Messaging-Steuerkomponente zu einem einzigen Cluster.

Nachfolgend wird die Vorgehensweise zur Konfiguration einer Vier-Cluster-Topologie mit IBM Business Process Manager für die Erstellung einer kombinierten IBM Business Process Manager- und IBM Business Monitor-Implementierungsumgebung beschrieben:

1. Führen Sie die Schritte zur Installationsvorbereitung im Abschnitt 'Installation vorbereiten' aus.
2. Installieren Sie das IBM BPM-Produkt. Erstellen Sie kein Entwicklungsprofil.
3. Installieren Sie IBM Monitor in der BPM WAS-Umgebung.
4. Erstellen Sie ein Deployment Manager-Profil mit dem Profile Management Tool oder mit dem Befehl `manageprofiles`, indem Sie die im Abschnitt 'Profile erstellen und erweitern' beschriebenen Schritte ausführen.
5. Erweitern Sie das Profil auf MONITOR-Deployment Manager.
6. Erstellen Sie ein angepasstes Profil für BPM, das später eingebunden wird.



7. Erweitern Sie das Profil auf angepasstes MONITOR-Profil.
8. Starten Sie das Deployment Manager-Profil.
9. Führen Sie den Befehl AddNode aus, um angepasste Profile zu erstellen, die in das Deployment Manager-Profil eingebunden werden.
10. Konfigurieren Sie die Implementierungsumgebung schrittweise, indem Sie das Vier-Cluster-Muster auswählen. Führen Sie die im Abschnitt 'Implementierungsumgebung mit einem Muster erstellen' beschriebenen Schritte aus.

Die Cluster werden erstellt und alle erforderlichen IBM Business Monitor- und IBM BPM-Komponenten werden automatisch installiert und konfiguriert.

Optional können Sie den Status der Komponenten überprüfen und über den Konfigurationsassistenten in der Administrationskonsole Aktualisierungen durchführen.

**Zugehörige Konzepte:**

„Vier-Cluster-Topologie“ auf Seite 7

Sie können IBM Business Monitor in viele Topologien installieren. Mit der Vier-Cluster-Topologie können Sie eine Hochleistungsumgebung einrichten.





---

## Kapitel 3. Installation vorbereiten

Stellen Sie vor der Installation von IBM Business Monitor sicher, dass die erforderlichen Hardware- und Softwarevoraussetzungen erfüllt sind. In einigen Betriebsumgebungen sind besondere Vorbereitungen erforderlich, damit Sie installieren können.

---

### Hardware- und Softwarevoraussetzungen

IBM Business Monitor kann unter den Betriebssystemen AIX, Windows, Linux, Linux on zSeries, Solaris und z/OS ausgeführt werden.

Informationen zu den aktuellsten Hardware- und Softwareanforderungen finden Sie im Thema Systemanforderungen für IBM Business Monitor.

Diese Links umfassen unterstützte LDAP-Server. Eigenständige LDAP-Registries werden ebenfalls von IBM Business Monitor unterstützt. Alle folgenden Typen werden als aktuelle Realmdefinitionen für das aktuelle Benutzeraccountrepository unterstützt:

- Eingebundene Repositorys
- Lokales Betriebssystem
- Eigenständige LDAP-Registry
- Eigenständige angepasste Registry

---

### Betriebssysteme für die Produktinstallation vorbereiten

Vor der Installation von IBM Business Monitor müssen Sie Ihr Betriebssystem vorbereiten. Die Konfiguration ist abhängig vom Typ des von Ihnen verwendeten Betriebssystems.

Führen Sie die folgenden Tasks aus, bevor Sie die Installationsumgebung vorbereiten:

- Inaktivieren Sie die Firewall, wenn auf dem System, auf dem IBM Business Monitor installiert werden soll, eine Firewall ausgeführt wird.
- Stellen Sie sicher, dass Ihnen über Ihre Benutzeranmeldung ein Zugriff auf Ihre DB2- oder Oracle-Datenbankbefehle erteilt wird.
- Führen Sie die zusätzlichen Tasks für Ihr Betriebssystem aus.

### AIX-Systeme für die Installation vorbereiten

Bevor Sie IBM Business Monitor installieren können, müssen Sie Ihr Betriebssystem AIX vorbereiten.

Da WebSphere Application Server eine Voraussetzung für IBM Business Monitor ist, müssen Sie die erforderlichen Vorbereitungsschritte ausführen, die im Abschnitt Betriebssystem für die Produktinstallation vorbereiten im Information Center von WebSphere Application Server beschrieben sind.

Da bestimmte Schritte für eine Version des Betriebssystems spezifisch sind, gelten für Ihre Umgebung möglicherweise nicht alle Schritte. Wenn ein bestimmter Schritt nicht speziell markiert ist, führen Sie den Schritt für alle Versionen des Betriebssystems aus.

Im folgenden technischen Hinweis finden Sie weitere Vorbereitungsinformationen zur Konfiguration von Installation Manager zur Ausführung auf 64-Bit-AIX-Systemen: <https://www-304.ibm.com/support/docview.wss?uid=swg21330190&wv=1>

Führen Sie die folgenden Schritte auf Ihrem AIX-System aus, bevor Sie IBM Business Monitor installieren:

1. Erhöhen Sie die maximale Anzahl geöffneter Dateien. Die Standardeinstellung ist in der Regel nicht ausreichend. Sie können die gegenwärtig festgelegte maximale Anzahl geöffneter Dateien mit dem Befehl `ulimit -n` prüfen. Das folgende Beispiel zeigt, wie die maximale Anzahl geöffneter Dateien auf 8800 erhöht wird. Dieser Wert ist für die meisten Systeme ausreichend. Die Anforderung für 'ulimit' wird bei der Installation dynamisch berechnet und sollte möglicherweise höher sein - abhängig von den von Ihnen ausgewählten Optionen.

Führen Sie vor der Installation den folgenden Befehl aus:

```
ulimit -n 8800
```

Alternativ können Sie die folgenden Schritte ausführen, um die Datei für Ressourcengrenzen zu bearbeiten:

- a. Öffnen Sie die Datei `/etc/security/limits`.
- b. Bearbeiten Sie den Abschnitt **default** bzw. fügen Sie diesen Abschnitt hinzu, um die folgende Zeile einzufügen:

```
nofiles = 8800
```

- c. Speichern und schließen Sie die Datei.
- d. Melden Sie sich vom Betriebssystem ab und melden Sie sich wieder an.

2. Setzen Sie den Wert für **umask** mit dem folgenden Befehl auf 022:

```
umask 022
```

3. Stellen Sie sicher, dass Mozilla Firefox mit Version 3.5.x.x (oder höher) installiert ist.
4. Erhöhen Sie vor dem Starten des Datenübertragungsservice die Anzahl der im Betriebssystem AIX konfigurierten Prozesse, um einen Fehler durch Zurücksetzen der Verbindung zu vermeiden. Sie können die Anzahl der Prozesse mit einem Befehl oder über die AIX-Schnittstelle erhöhen.

- Führen Sie den folgenden Befehl aus:

```
chgdev -l sys0 -a maxuproc='256'
```

- Geben Sie in der AIX-Schnittstelle **smitty** ein und wählen Sie dann **Systemumgebungen > Merkmale des Betriebssystems ändern/anzeigen > Pro Benutzer zulässige Prozesse (Anzahl) aus..**

5. Führen Sie die Schritte unter AIX-Systeme optimieren aus.

## Linux-Systeme für die Installation vorbereiten

Bevor Sie IBM Business Monitor installieren können, müssen Sie Ihr Linux-Betriebssystem vorbereiten.

Da WebSphere Application Server eine Voraussetzung für IBM Business Monitor ist, müssen Sie alle vorbereitenden Schritte ausführen, die im Information Center von WebSphere Application Server unter der Überschrift Betriebssystem für die Installation vorbereiten beschrieben werden.

Vergewissern Sie sich, dass Mozilla Firefox Version 3.5.x.x oder höher auf dem System installiert ist.

Da bestimmte Schritte sich nach der Version des Betriebssystems richten, gelten möglicherweise nicht alle Schritte für Ihre Umgebung. Wenn für einen bestimmten Schritt kein Qualifikationsmerkmal angegeben ist, bezieht sich der betreffende Schritt auf alle Versionen des Betriebssystems. Um Installation Manager auf Red Hat Enterprise Linux 6.0 (64-Bit) zu installieren, orientieren Sie sich an den Informationen in Installation Manager kann auf RHEL 6.0 (64-Bit) nicht installiert werden.

Führen Sie die folgenden Schritte auf Ihrem Linux-System aus, bevor Sie IBM Business Monitor installieren:

1. Wenn Sie planen, IBM Business Monitor unter Verwendung von DB2 Express unter Red Hat Enterprise Linux 6 zu installieren, stellen Sie sicher, dass der Benutzer über Administratorberechtigungen (Rootbenutzer) verfügt. Als Rootbenutzer müssen Sie außerdem sicherstellen, dass alle Kernelanforderungen erfüllt sind, bevor die Installation von DB2 Express beginnt. Sie können die aktuellen Werte lokalisieren, indem Sie eine Syntaxanalyse der Ausgabe des Befehls `ipcs -l` durchführen. Gehen Sie wie folgt vor, um die Werte zu ändern:
  - a. Fügen Sie die folgenden Zeilen in der hier angegebenen Reihenfolge zur Datei `/etc/sysctl.conf` hinzu:

```
kernel.shmni=4096
kernel.shmmax=4294967296
kernel.shmall=8388608
#kernel.sem=<SEMMS><SEMMNS><SEMOPM><SEMMNI>
kernel.sem=250 256000 32 4096
kernel.msgmni=16384
kernel.msgmax=65536
kernel.msgmnb=65536
```
  - b. Fügen Sie die folgenden Zeilen am Ende der Datei `/etc/security/limits.conf` hinzu:

```
# - stack - max stack size (KB)
* soft stack 32768
* hard stack 32768
# - nofile - max number of open files
* soft nofile 65536
* hard nofile 65536
# - nproc - max number of processes
* soft nproc 16384
* hard nproc 16384
```
  - c. Führen Sie einen Warmstart Ihres Systems durch.
2. Falls Sie NICHT beabsichtigen, IBM Business Monitor mit DB2 Express zu installieren, setzen Sie die maximale Anzahl offener Dateien herauf. Die Standardeinstellung ist in der Regel nicht ausreichend. Sie können die gegenwärtig festgelegte maximale Anzahl geöffneter Dateien mit dem Befehl `ulimit -n` prüfen. Das folgende Beispiel zeigt, wie die maximale Anzahl geöffneter Dateien auf 8800 erhöht wird. Dieser Wert ist für die meisten Systeme ausreichend. Die Anforderung für 'ulimit' wird bei der Installation dynamisch berechnet und sollte möglicherweise höher sein - abhängig von den von Ihnen ausgewählten Optionen.
  - a. Öffnen Sie die Datei `/etc/security/limits.conf`.
  - b. Suchen Sie den Parameter `nofile` und erhöhen Sie den Wert. Wenn keine Zeile mit dem Parameter `nofile` vorhanden ist, fügen Sie der Datei die folgenden Zeilen hinzu:

```
* hard nofile 8800
```

```
* soft nofile 8800
```

- c. Speichern und schließen Sie die Datei.
- d. Melden Sie sich ab und wieder an.

Weitere Informationen zu dieser Einstellung erhalten Sie, wenn Sie man `limits.conf` ausführen. Sie können aber auch den Abschnitt Betriebssysteme für die Produktinstallation vorbereiten im Information Center von WebSphere Application Server lesen.

3. Installieren Sie die folgenden Pakete für Ihr Betriebssystem:

Option	Bezeichnung
Red Hat Enterprise Linux 4	compat-libstdc++-33-3.2.3-47.3 compat-db-4.1.25-9 xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2 rpm-build-4.3.3-7.nonptl compat-libstdc++-296-2.96-132.7.2
Red Hat Enterprise Linux 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 rpm-build-4.4.2-37.el5 <b>Nur 64-Bit-Kernel:</b> compat-libstdc++-296-2.96-138
Red Hat Enterprise Linux 6	Korn-Shell ksh-version.rpm  Detaillierte Anweisungen und eine Liste der Pakete finden Sie unter Unable to install Installation Manager on RHEL 6.0 (64-bit).
SUSE Linux Enterprise Server 9.0	XFree86-libs-32bit-9 glibc-32bit-9 glib-32bit-9 gtk-32bit-9

Sie können auch ein späteres Release dieser Pakete installieren, wenn neue Pakete als Errata verfügbar sind. Wenn weitere Pakete vorhanden sind, die speziell für Ihre Hardware benötigt werden, dann installieren Sie sie jetzt.

Sie können Abhängigkeiten (alle erforderlichen Pakete) durch einzeilige Befehle installieren. Die folgenden Beispiele zeigen Befehle mit Standardpaketmanagern auf unterstützten Linux-Varianten.

- **Red Hat Enterprise Linux 5 (32-Bit):**

```
yum install compat-libstdc++-33 compat-db libXp rpm-build RHEL 5.x
```

- **Red Hat Enterprise Linux 5 (64-Bit):**

```
yum install compat-libstdc++-33 compat-db libXp rpm-build compat-libstdc++-296
```

- **SUSE Linux:**

```
zypper install XFree86-libs-32bit-9 glibc-32bit-9 glib-32bit-9 gtk-32bit-9
```

4. Setzen Sie den Wert für **umask** mit dem folgenden Befehl auf 022:

```
umask 022
```

5. Auf Red Hat Enterprise Linux 5-Systemen: Inaktivieren Sie SELinux oder versetzen Sie SELinux in einen toleranten Modus.
6. Starten Sie den Computer erneut.

7. Führen Sie die Schritte unter Linux-Systeme optimieren aus.

## Solaris-Systeme für die Installation vorbereiten

Vor der Installation von IBM Business Monitor müssen Sie Ihr Solaris-Betriebssystem vorbereiten.

Da WebSphere Application Server eine Voraussetzung für IBM Business Monitor ist, müssen Sie die erforderlichen Vorbereitungsschritte ausführen, die im Abschnitt Betriebssystem für die Produktinstallation vorbereiten im Information Center von WebSphere Application Server beschrieben sind.

Die HotSpot Java JVM wurde von Sun Microsystems für das Betriebssystem Solaris entwickelt. Die Java-Java-Heapspeicherstruktur und -verwaltung für die HotSpot JVM weicht von der für andere Java Virtual Machines (JVMs) ab. In Ihrer Umgebung besteht unter Umständen die Notwendigkeit, die Heapspeicherverwaltung der JVM zu optimieren, um Fehler des Typs `java.lang.OutOfMemoryError: PermGen` während der Profilerstellung oder Serverlaufzeit zu optimieren. Möglicherweise ist es erforderlich, den Wert für den JVM-Parameter **MaxPermSize** zu aktualisieren.

Da bestimmte Schritte sich nach der Version des Betriebssystems richten, gelten möglicherweise nicht alle Schritte für Ihre Umgebung. Wenn für einen bestimmten Schritt kein Qualifikationsmerkmal angegeben ist, bezieht sich der betreffende Schritt auf alle Versionen des Betriebssystems.

Führen Sie die folgenden Schritte auf Ihrem Solaris-System vor der Installation von IBM Business Monitor aus:

1. Erhöhen Sie den Wert für die maximale Anzahl geöffneter Dateien. Die Standardeinstellung ist in der Regel zu niedrig. Sie können den aktuellen Wert für die maximale Anzahl offener Dateien überprüfen, indem Sie `ulimit -n` eingeben. Das folgende Beispiel zeigt eine Erhöhung des Werts für die maximale Anzahl geöffneter Dateien auf 8800. Dieser Wert ist für die meisten System ausreichend groß. Die Anforderung "ulimit" wird zum Installationszeitpunkt dynamisch errechnet und sollte je nach den gewählten Optionen unter Umständen höher liegen.

Führen Sie vor Beginn der Installation den folgenden Befehl aus:

```
ulimit -Hn 8800
```

Alternativ dazu können Sie die folgenden Schritte ausführen, um die Datei mit Ressourcengrenzwerten zu bearbeiten:

- a. Öffnen Sie `/etc/system`.
- b. Fügen Sie am Dateiende die folgende Zeile hinzu:

```
set rlim_fd_max=8800
```
- c. Speichern Sie die Datei, und schließen Sie sie wieder.
- d. Melden Sie sich beim Betriebssystem ab und anschließend wieder an.

2. Setzen Sie mit folgendem Befehl den Wert von **umask** auf Wert 022:

```
umask 022
```

3. Führen Sie die Schritte unter Solaris-Systeme optimieren aus.

Bevor Sie IBM Business Monitor-Profilen auf Ihrem Solaris-System erstellen oder erweitern, ändern Sie den JVM-Parameter **MaxPermSize**, indem Sie die Schritte in `OutOfMemoryErrors`-Fehler bei der Profilerstellung unter Solaris vermeiden ausführen.

## Windows-Systeme für die Installation vorbereiten

Vor der Installation von IBM Business Monitor müssen Sie Ihr Windows-Betriebssystem vorbereiten.

Da WebSphere Application Server ein vorausgesetztes Produkt für IBM Business Monitor ist, müssen Sie alle vorbereitenden Tasks für WebSphere Application Server ausführen, bevor Sie IBM Business Monitor installieren.

Führen Sie die folgenden Schritte auf Ihrem Windows-System vor der Installation von IBM Business Monitor aus:

1. Führen Sie die Schritte aus, die im Abschnitt Windows-Systeme für die Installation vorbereiten im Information Center von WebSphere Application Server beschrieben sind.
2. Führen Sie die Schritte unter Windows-Systeme optimieren aus.

---

## Kapitel 4. IBM Business Monitor-Software installieren

Sie können IBM Business Monitor im Dialogbetrieb oder im unbeaufsichtigten Modus installieren. Sie können IBM Business Monitor mit anderen Softwareprodukten in Ihrer Überwachungs Umgebung verwenden, z. B. mit WebSphere Portal oder Process Server.

Bei einer Installation von IBM Business Monitor im Dialogbetrieb müssen Sie den Installation Manager verwenden, und zwar unabhängig davon, ob Sie alle IBM Business Monitor-Komponenten auf einem einzigen Server oder in Clustern in einer Network Deployment-Umgebung installieren.

Alternativ können Sie vorab eine Antwortdatei definieren und IBM Business Monitor über eine Befehlszeile im unbeaufsichtigten Modus installieren, ohne dass ein Dialog mit dem IBM Business Monitor-Installationsprogramm erforderlich ist.


---

### Über das Produkt-Launchpad installieren

Mit dem Launchpadprogramm des Produkts IBM Business Monitor steht Ihnen ein zentraler Ort zum Anzeigen von Releaseinformationen für IBM Business Monitor, zum Installieren von WebSphere Application Server (falls erforderlich) und zum Starten des Installationsprozesses zur Verfügung.

Führen Sie, falls noch nicht geschehen, die vor der Installation erforderlichen Aufgaben aus, die im Abschnitt Kapitel 3, „Installation vorbereiten“, auf Seite 35 beschrieben werden.

Angaben zu den Standardinstallationspositionen finden Sie im zugehörigen Verweis.



 Zum Installieren oder Ausführen von IBM Business Monitor unter Windows 7, Windows Vista oder Windows Server 2008 müssen Sie die Berechtigungen Ihres Microsoft Windows-Benutzerkontos hochstufen. Klicken Sie unabhängig davon, ob Sie als Benutzer mit oder ohne Verwaltungsaufgaben arbeiten, mit der rechten Maustaste auf die Datei `launchpad.exe` und wählen Sie die Option **Als Administrator ausführen** aus.

Verwenden Sie in folgenden Fällen das Launchpadprogramm des Produkts, um die Installation von IBM Business Monitor zu starten:

- Bei der Installation von den Produkt-DVDs
- Bei der Installation aus einem elektronischen Installationsimage im lokalen Dateisystem
- Bei der Installation aus einem elektronischen Installationsimage auf einem gemeinsam genutzten Laufwerk

Gehen Sie wie folgt vor, um das Launchpadprogramm zu starten und WebSphere Application Server zu installieren (falls noch nicht geschehen). Sie können gleichzeitig jeweils nur ein einziges Launchpad ausführen.




1. Legen Sie die erste IBM Business Monitor-DVD in das DVD-Laufwerk ein.

  Stellen Sie sicher, dass das DVD-Laufwerk angehängt ist.



2. Wenn die automatische Ausführung auf dem System aktiviert ist, wird das Launchpadprogramm von IBM Business Monitor automatisch geöffnet. Falls nicht, gehen Sie wie folgt vor:
  - Führen Sie die Datei `launchpad.sh` aus, die sich im Stammverzeichnis der DVD befindet.
  - Führen Sie die Datei `launchpad.exe` aus, oder bei einem 64-Bitsystem `launchpad64.exe`, die sich jeweils im Stammverzeichnis der DVD befindet.
3. Optional: Wenn eine Nachricht angezeigt wird, die Sie dazu auffordert, das Launchpad zu aktualisieren, klicken Sie auf **Aktualisieren**, um die neuesten Updates abzurufen. Die Updates werden installiert und es erfolgt ein automatischer Neustart Ihres Launchpads.

Wenn Sie nicht auf das Internet zugreifen können und die Updates für das Launchpad von einem lokalen Verzeichnis aus installieren möchten, können Sie Installation Manager über eine Eigenschaftendatei mitteilen, an welcher Position sich die Updates befinden. Erstellen Sie die folgende Datei:

-   `/home/user/bpm_updates.properties`
-  `C:\HOMEPATH\bpm_updates.properties`

Unter Windows 7, Windows Vista und Windows Server 2008 wird von der Umgebungsvariablen `HOMEPATH` auf `C:\Users\benutzername\` verwiesen.

Weitere Informationen zu Updates für Installation Manager finden Sie unter Installation Manager updates.

**Anmerkung:** Stellen Sie sicher, dass Sie einen Schreib-/Lesezugriff auf die in der Datei `bpm_updates.properties` angegebenen Ordner besitzen.

Die Datei verwendet ein Launchpad-Präfix, auf das ein Punkt folgt. Der Bestandteil des Namens nach dem Präfix und dem Punkt kann eine beliebige Zeichenfolge sein; so können Sie auf mehrere Positionen für Launchpad-Updates verweisen. Die Positionen können entweder lokale Verzeichnisse oder URLs sein. Beispiel:

```
launchpad.1=http://test/launchpad
launchpad.2=C:\launchpad_updates
```

4. Optional: Klicken Sie auf **Help System installation** (Hilfesysteminstallation), um die Produkthilfe und dokumentation auf Ihrem Rechner zu installieren. Bei dem Hilfesystem handelt es sich um ein Eclipse-Framework zur Anzeige der Dokumentation.
5. Wenn Sie unter Windows der Administratorgruppe angehören oder wenn Sie ein Rootbenutzer auf einem Linux- oder UNIX-System sind, dann vergewissern Sie sich, dass **Install as administrative user** (Als Benutzer mit Verwaltungsaufgaben installieren) ausgewählt ist. Wählen Sie dieses Kontrollkästchen nur ab, wenn Sie kein Benutzer mit Verwaltungsaufgaben sind oder wenn Sie die Installation unter Ihrem eigenen Benutzernamen durchführen wollen, ohne anderen Benutzern Berechtigungen zu erteilen.
6. **Wenn WebSphere Application Server noch nicht installiert ist**, klicken Sie auf die Schaltfläche **Installieren**, um die Installation von IBM Business Monitor zu starten.

**Wichtig:** Wenn Sie auf einem 64-Bit-System arbeiten, erhalten Sie unter Umständen folgende Nachricht:

Die Prüfung der erforderlichen Systemvoraussetzungen für das Launchpad ist auf Ihrem Betriebssystem



Wenn Sie diese Meldung sehen, hat Ihr Server die 32-Bit-Version der GTK-Bibliothek nicht installiert, oder die Bibliothek liegt nicht in der richtigen Version vor. Aktualisieren Sie den Server mit der richtigen Version der 32-Bit-GTK-Bibliothek von einer DVD oder der offiziellen Website Ihres Betriebssystems, bevor Sie mit der Installation fortfahren.

Der Installation Manager wird gestartet und automatisch konfiguriert. Gehen Sie zum Abschnitt „IBM Business Monitor im Dialogbetrieb installieren“ auf Seite 44 mit den weiteren Installationsanweisungen.

7. **Wenn Sie IBM Business Monitor auf einer vorhandenen Installation von WebSphere Application Server installieren möchten, klicken Sie auf **Installation on existing WebSphere Application Server**** (Auf vorhandenem WebSphere Application Server installieren).
  - a. Wenn Sie unter Windows der Administratorgruppe angehören oder wenn Sie ein Rootbenutzer auf einem Linux- oder UNIX-System sind, dann vergewissern Sie sich, dass **Install as administrative user** (Als Benutzer mit Verwaltungsaufgaben installieren) ausgewählt ist. Wählen Sie dieses Kontrollkästchen nur ab, wenn Sie kein Benutzer mit Verwaltungsaufgaben sind oder wenn Sie die Installation unter Ihrem eigenen Benutzernamen durchführen wollen, ohne anderen Benutzern Berechtigungen zu erteilen.
  - b. Klicken Sie auf **Import or Update** (Importieren oder Aktualisieren).
    - Wenn das Fenster zum Öffnen einer Datei angezeigt wird, klicken Sie auf **Run** (Ausführen). Der Installation Manager wird geöffnet.
    - Klicken Sie auf **Import** (Importieren), um WebSphere Application Server in den Installation Manager zu importieren. Sie müssen WebSphere Application Server importieren, wenn dieses Produkt noch niemals auf Ihr System importiert wurde oder wenn es mit dem Update Installer aktualisiert wurde, nachdem es zuletzt importiert wurde.
    - Klicken Sie auf **Browse** (Durchsuchen) und wählen Sie das Verzeichnis aus, in dem WebSphere Application Server installiert wurde, z. B. `application_server-stammverzeichnis`.
    - Klicken Sie auf **Next** (Weiter) und dann auf **Import** (Importieren).
    - Klicken Sie auf **Finish** (Fertig stellen).
    - Klicken Sie im Installation Manager-Fenster auf **Update** (Aktualisieren).
    - Wählen Sie die Paketgruppe **IBM WebSphere Application Server - ND** aus.
  - c. Klicken Sie auf **Install** (Installieren), um die Installation von IBM Business Monitor zu starten. Wenn das Fenster 'Open file' (Datei öffnen) angezeigt wird, klicken Sie auf **Run** (Ausführen).

**Tipp:** Wählen Sie auf der Seite 'Update Packages' (Aktualisierungspakete) die Option **Show All** (Alle anzeigen) an, um die verfügbaren Updates anzuzeigen.

- Klicken Sie auf **Weiter** und folgen Sie den Anweisungen auf den einzelnen Seiten. Übernehmen Sie dabei jeweils die Standardwerte.
- Schließen Sie den Installation Manager und kehren Sie zur Launchpad-Anwendung zurück.

**Wichtig:** Wenn Sie auf einem 64-Bit-System arbeiten, erhalten Sie unter Umständen folgende Nachricht:

Die Prüfung der erforderlichen Systemvoraussetzungen für das Launchpad ist auf Ihrem Betrie...

Wenn Sie diese Meldung sehen, hat Ihr Server die 32-Bit-Version der GTK-Bibliothek nicht installiert, oder die Bibliothek liegt nicht in der richtigen

Version vor. Aktualisieren Sie den Server mit der richtigen Version der 32-Bit-GTK-Bibliothek von einer DVD oder der offiziellen Website Ihres Betriebssystems, bevor Sie mit der Installation fortfahren.

- d. Klicken Sie auf **Install IBM Business Monitor** (IBM Business Monitor installieren). Der Installation Manager wird gestartet und automatisch konfiguriert. Gehen Sie zum Abschnitt „IBM Business Monitor im Dialogbetrieb installieren“ mit den weiteren Installationsanweisungen.

Sofern Ihr Betriebssystem dies unterstützt, können Sie im Launchpad auf **Help System Installation** (Hilfesysteminstallation) klicken, um das Information Center zu installieren.

## IBM Business Monitor im Dialogbetrieb installieren

Sie können IBM Business Monitor im Dialogbetrieb mit dem Installation Manager installieren. Dies gilt sowohl für die Installation aller Komponenten auf einem einzelnen Server als auch für die Installation der Komponenten in Clustern in einer Network Deployment-Umgebung.

Starten Sie den Installation Manager über das Produkt-Launchpad. Angaben zu den Standardinstallationspositionen finden Sie im zugehörigen Linkverweis.

Gehen Sie zum Installieren von IBM Business Monitor wie folgt vor:

1. Klicken Sie auf der **Startseite** von Installation Manager auf **Installationspakete** und anschließend auf **Weiter**, um fortzufahren. Daraufhin werden die folgenden Pakete ausgewählt:

### IBM Cognos Business Intelligence

Entfernen Sie den Haken aus dem Markierungsfeld, falls Sie derzeit Microsoft Windows verwenden und kein Benutzer mit Verwaltungsaufgaben sind.

### WebSphere Application Server - ND

Entfernen Sie den Haken aus diesem Markierungsfeld, wenn das Paket bereits installiert ist.

### DB2 Express

Entfernen Sie den Haken aus diesem Markierungsfeld, wenn bereits eine Datenbank vorhanden ist, die Sie verwenden möchten oder wenn Sie kein Benutzer mit Verwaltungsaufgaben sind.

### IBM Business Monitor

Wenn Sie bei der Prüfung der Voraussetzungen die folgende Warnung erhalten, führen Sie die nachfolgend beschriebenen plattformspezifischen Schritte aus, um den Wert für `ulimit` zu erhöhen.

Auf dem aktuellen System wurde für die Einstellung 'ulimit' ein Wert unterhalb des empfohlenen Werts *empfohlener\_wert* festgestellt. Erhöhen Sie den Wert von 'ulimit' auf den *empfohlener\_wert* und wiederholen Sie die Installation.

Beenden Sie das Installationsprogramm. Wenn Sie der Rootbenutzer sind, öffnen Sie eine Eingabeaufforderung und starten Sie dann das Installationsprogramm erneut. Wenn Sie ein Benutzer ohne Rootberechtigung sind, kontaktieren Sie den Systemadministrator, damit dieser mithilfe des Befehls 'ulimit -n *empfohlener\_wert*' die Änderung vornimmt, und starten Sie dann das Installationsprogramm erneut.

Die Berechnung des erforderlichen Werts erfolgt auf der Basis der Version von WebSphere Application Server und der Konfiguration, die Sie installieren.

- a. Legen Sie die maximale Anzahl geöffneter Dateien mithilfe der folgenden Schritte fest: 



- 1) Öffnen Sie die Datei `/etc/security/limits.conf`.
  - 2) Suchen Sie den Parameter `nofile` und erhöhen Sie den Wert. Wenn keine Zeile mit dem Parameter `nofile` vorhanden ist, fügen Sie der Datei die folgenden Zeilen hinzu:
    - \* `hard nofile empfohlener_wert`
    - \* `soft nofile empfohlener_wert`
  - 3) Speichern und schließen Sie die Datei.
  - 4) Melden Sie sich ab und wieder an.
- b. Starten Sie den Computer erneut.
- c. Starten Sie das Installationsprogramm erneut.

2. Lesen Sie die Lizenzvereinbarung für das ausgewählte Paket auf der Seite **Lizenzen**.

Wenn Sie mehr als ein Paket zur Installation ausgewählt haben, gibt es unter Umständen für jedes Paket eine eigene Lizenzvereinbarung. Klicken Sie links auf der **Lizenz**-Seite auf jede Paketversion, damit deren Lizenzvereinbarung angezeigt wird. Die Paketversionen, die Sie zur Installation ausgewählt haben (z.B. das Basispaket und das Update) werden unter dem Paketnamen aufgeführt.

- a. Wenn Sie den Bedingungen aller Lizenzvereinbarungen zustimmen, klicken Sie auf **Ich akzeptiere die Bedingungen der Lizenzvereinbarungen**.
  - b. Klicken Sie auf **Weiter**.
3. Wenn es sich bei IBM Business Monitor um das erste Paket handelt, das mithilfe von Installation Manager installiert wird, geben Sie den Pfad für das *Verzeichnis für gemeinsam genutzte Ressourcen* im Feld **Verzeichnis für gemeinsam genutzte Ressourcen** auf der Seite **Speicherposition** manuell ein, oder Sie akzeptieren den Standardpfad. Das Verzeichnis für gemeinsam genutzte Ressourcen enthält Ressourcen, die von einer oder mehreren Paketgruppen gemeinsam genutzt werden können.

**Wichtig:**

- a. Sie können das Verzeichnis für gemeinsam genutzte Ressourcen nur angeben, wenn Sie ein Paket das erste Mal installieren. Verwenden Sie dafür Ihre größte Festplatte, damit ausreichend Platz für gemeinsame Ressourcen zukünftiger Pakete bereitgestellt wird. Sie können die Verzeichnissposition nicht ändern, außer wenn Sie alle Pakete deinstallieren.
- b. Stellen Sie sicher, dass Ihr Installationsverzeichnispfad keine runden Klammern enthält.
- c.   Stellen Sie sicher, dass Ihr Installationsverzeichnispfad keine Leerzeichen enthält.

Klicken Sie auf **Weiter**.

4. Auf der nächsten Seite **Speicherposition** können Sie eine *Paketgruppe* erstellen, in das das IBM Business Monitor-Paket installiert wird. Führen Sie die folgenden Schritte aus, um eine neue Paketgruppe zu erstellen:
- a. Wählen Sie **Neue Paketgruppe erstellen** aus.
  - b. Geben Sie den Pfad für das Installationsverzeichnis der Paketgruppe ein. Stellen Sie sicher, dass Ihr Installationsverzeichnispfad keine runden Klammern enthält. Verwenden Sie keine Leerzeichen im Verzeichnispfad. Der Name der Paketgruppe wird automatisch generiert.
  - c. Klicken Sie auf **Weiter**.

Der Assistent zur Installation von Paketen zeigt eine Nachricht an, wenn aktive Prozesse (z. B. der WebSphere Application Server-Server) erkannt werden. Wenn die Nachricht angezeigt wird, klicken Sie auf **Abbrechen**, beenden Sie den aktiven Prozess und beginnen Sie erneut mit der Installation.

5. Wählen Sie auf der Seite **Features** (Komponenten) die Paketfeatures aus, die Sie installieren möchten.
  - a. Optional: Wenn Sie die Abhängigkeitsbeziehungen zwischen Features sehen möchten, aktivieren Sie das Kontrollkästchen **Abhängigkeiten anzeigen**.
  - b. Optional: Klicken Sie auf ein Feature, um unter **Details** die zugehörige Kurzbeschreibung anzuzeigen.
  - c. Wählen Sie Features im Paket aus oder ab. Installation Manager erzwingt automatisch Abhängigkeiten mit anderen Features und zeigt die aktuelle Größe des Downloads und den erforderlichen Plattenspeicherplatz für die Installation an.
    - Falls Sie keine Features auswählen, werden die Lizenzdateien für Business Space und IBM Business Monitor installiert.
    - Wenn Sie **Business Monitor Server** erweitern und ein oder mehrere eigenständige Entwicklungsprofile auswählen, werden diese während der Installation für Sie erstellt. Um Entwicklungsprofile für Process Server oder WebSphere Enterprise Service Bus erstellen zu können, müssen diese Pakete bereits installiert sein.

Ein eigenständiges Entwicklungsprofil ist ein Standardentwicklungsprofil, das eine IBM Business Monitor-Testumgebung bereitstellt. Bei dem Entwicklungsprofil für Process Server ist zudem Business Process Rules Manager aktiviert. Um ein eigenständiges Entwicklungsprofil zu erstellen, müssen Sie die Verwaltungssicherheitsberechtigungsanzeige (Benutzername und Kennwort) für den zu erstellenden Server angeben.

Die Verwendung eines eigenständigen Entwicklungsprofils in einer Produktionsumgebung ist nicht möglich. Wenn Sie kein eigenständiges Standardentwicklungsprofil installieren möchten, können Sie die Installation zu einem späteren Zeitpunkt durchführen, indem Sie den Installation Manager starten und auf der ersten Seite auf **Ändern** klicken.

Wenn Sie **Business Monitor Server** 8.0 installieren und bereits über früher erstellte Profile verfügen, bleiben diese Profile automatisch erhalten. Sie müssen sie nicht neu erstellen.
  - d. Erforderlich: Wählen Sie das WebSphere Application Server-Feature EJBDeploy-Tool für EJB-Module vor EJB 3.0 aus. Dieses Feature ist standardmäßig ausgewählt. Wenn es nicht ausgewählt ist, funktionieren einige Komponenten von **Business Monitor Server** 8.0 möglicherweise nicht ordnungsgemäß.
  - e. Klicken Sie nach der Auswahl der Features auf **Weiter**.
6. Wenn Sie ein eigenständiges Entwicklungsprofil ausgewählt haben, müssen Sie auf der Seite **Profile** die Berechtigungsanzeige für Ihr Profil eingeben. Der Standardbenutzername lautet `admin` und das Standardkennwort heißt `admin`.
7. Geben Sie auf der Seite **Gemeinsame Konfigurationen** die Berechtigungsanzeige für die Datenbank ein, falls Sie bereits über eine Datenbank verfügen. Wenn Sie DB2 Express ausgewählt haben, müssen Sie einen Benutzernamen und ein Kennwort für DB2 eingeben. Der Standardname des Benutzers mit Verwaltungsaufgaben lautet `bpmadmin`. Wählen Sie ein Kennwort, das die Kennwortrichtlinie Ihres Systems (z. B. Windows 2008) einhält.

**Einschränkung:** Benutzernamen dürfen keine landessprachlichen Zeichenfolgen enthalten.

Klicken Sie auf **Weiter**.

8. Überprüfen Sie auf der Seite **Zusammenfassung** Ihre Auswahl, bevor Sie das IBM Business Monitor-Paket installieren.
  - Wenn Sie die Auswahl, die Sie auf vorherigen Seiten getroffen haben, ändern möchten, klicken Sie auf **Zurück** und nehmen Sie die gewünschten Änderungen vor.
  - Wenn die ausgewählten Installationsoptionen Ihren Vorstellungen entsprechen, klicken Sie zur Installation des Pakets auf **Installieren**.

Ein Fortschrittsanzeiger zeigt den Verlauf der Installation als Prozentsatz an.

9. Nach Abschluss des Installationsprozesses wird in einer Nachricht der Erfolg des Prozesses bestätigt. Wenn Sie sich dafür entschieden haben, bei der Installation ein eigenständiges Entwicklungsprofil zu erstellen, bzw. das Profil nicht vollständig erstellt wurde, wird Ihnen eine Fehlermeldung angezeigt, die Ihnen die Speicherposition des Fehlerprotokolls über die Profilerstellung `unterapplication_server-stammverzeichnis/logs/manageprofiles/profilname_create.log` angibt. Sie müssen zunächst das Profilerstellungsproblem beheben und mithilfe des Profile Management Tools bzw. dem Befehl **manageprofiles** ein Profil erstellen.
  - a. Optional: Klicken Sie auf **Protokolldatei anzeigen**, um die Installationsprotokolldatei für die aktuelle Sitzung in einem neuen Fenster zu öffnen. Sie müssen das Fenster 'Installationsprotokoll' auswählen, um fortfahren zu können.
  - b. Wählen Sie unter **Welches Programm möchten Sie starten?** aus, ob das Profile Management Tool beim Beenden gestartet werden soll. Wenn Sie bereits ein eigenständiges Entwicklungsprofil eingerichtet haben, können **Kein** auswählen. Für die Produktion müssen Sie mithilfe des Profile Management Tools oder des Befehls **manageprofiles** ein eigenständiges Serverprofil oder einen Deployment Manager definieren. Verwenden Sie hierzu die Informationen über das *Erstellen und Erweitern von Profilen*.
  - c. Klicken Sie auf **Fertig stellen**, um den Installation Manager zu schließen.

Für die Produktion müssen Sie mithilfe des Profile Management Tools oder des Befehls **manageprofiles** ein Profil für einen eigenständigen Server oder einen Deployment Manager erstellen.

**Einschränkung:** Wenn Sie während der Installation ein eigenständiges Entwicklungsprofil erstellt haben, ist zu beachten, dass es in einer Produktionsumgebung nicht funktioniert. Es dient dazu, Sie mit IBM Business Monitor vertraut zu machen, ohne ein funktionierendes Produktionsprofil erstellen zu müssen. Sie können das Profil über dessen Einstiegskonsolle starten.

- Öffnen Sie ein Befehlsfenster. Wechseln Sie in das Verzeichnis `profil-stammverzeichnis/firststeps.wbm` und führen Sie den Befehl `firststeps.sh` aus.
- Rufen Sie **Start > Alle Programme > IBM > Business Monitor 8.0 > Profile > profilname > Erste Schritte** auf.
- Wechseln Sie zu `profil-stammverzeichnis\firststeps.wbm` und führen Sie den Befehl `firststeps.bat` aus.

**Wichtig:** Um die Einführung (Erste Schritte, First Steps) unter Microsoft Windows 7, Microsoft Windows Vista, oder Microsoft Windows Server 2008 zu installieren oder auszuführen, müssen Sie Ihre Benutzerkontoberechtigungen für Mi-

Microsoft Windows erweitern, indem Sie mit der rechten Maustaste auf `firststeps.bat` klicken und **Run as administrator** (im Administratormodus ausführen) auswählen. Dies ist sowohl für Administratoren als auch für Benutzer ohne Administratorrechte erforderlich.

---

## IBM Business Monitor unbeaufsichtigt installieren

Sie können das IBM Business Monitor-Produktpaket im *unbeaufsichtigten* Installationsmodus installieren. Bei der Installation im unbeaufsichtigten Modus ist die Benutzerschnittstelle nicht verfügbar.

**Wichtig:** Zur Installation mehrerer Instanzen von IBM Business Monitor wird nur eine einzige IBM Installation Manager-Instanz benötigt.

### Unbeaufsichtigte Installation von IBM Business Monitor über die Befehlszeile

Sie können IBM Business Monitor über die Befehlszeile installieren.

Vor der Installation von IBM Business Monitor sollten Sie die Systemanforderungen des Produkts prüfen.

Die vorausgesetzten Betriebssystem- und Softwareversionen sind besonders wichtig. Auch wenn der Installationsprozess automatisch eine Überprüfung auf vorausgesetzte Betriebssystemprogrammkorrekturen durchführt, sollten Sie die Systemanforderungen überprüfen (falls noch nicht geschehen). Der Link zu den Systemanforderungen listet alle unterstützten Betriebssysteme sowie die Fixes und Patches für die Betriebssysteme auf, die Sie installieren müssen, damit Ihr Betriebssystem kompatibel ist. Es werden auch die erforderlichen Versionen aller Softwarevoraussetzungen aufgeführt.

Wenn Sie planen, IBM Business Monitor unter Verwendung von DB2 Express unter Red Hat Enterprise Linux 6 zu installieren, stellen Sie sicher, dass der Benutzer über Administratorberechtigungen (Rootbenutzer) verfügt. Als Rootbenutzer müssen Sie außerdem sicherstellen, dass alle Kernelanforderungen erfüllt sind, bevor die Installation von DB2 Express beginnt. Sie können die aktuellen Werte lokalisieren, indem Sie die Ausgabe des Befehls `ipcs -l` analysieren.

Wenn Sie nicht über die für die Installation von IBM Business Monitor erforderlichen Basisprodukte verfügen, müssen Sie sie im Rahmen der unbeaufsichtigten Installation mitinstallieren. Folgende Basisprodukte sind erforderlich:

- Installation Manager
- WebSphere Application Server Network Deployment

Die unbeaufsichtigte Installation führt die folgenden Tasks aus:

- Installation von Installation Manager, falls das Produkt noch nicht installiert wurde, oder Aktualisierung des Produkts auf die geeignete Version, falls es bereits installiert ist.
- Die erforderlichen Basisprodukte sowie IBM Business Monitor werden installiert.

Gehen Sie wie folgt vor, um IBM Business Monitor im unbeaufsichtigten Modus zu installieren:

1. Führen Sie den folgenden Befehl aus, um mit IBM Installation Manager verschlüsselte Kennwörter zu generieren, damit sichere Verbindungen zu DB2 und zur WebSphere-Administrationskonsole hergestellt werden können.



**Wichtig:** Wenn Sie Windows 7, Windows Vista oder Windows Server 2008 verwenden, starten Sie die Eingabeaufforderung, indem Sie mit der rechten Maustaste klicken und die Option **Als Administrator ausführen** auswählen.

Windows

```
IM-position\eclipse\tools\imutilsc -silent -nosplash encryptString zu_verschlüsselndes_kenwor
```

Linux

```
IM-position/eclipse/tools/imutilsc -silent -nosplash encryptString zu_verschlüsselndes_kenwor
```

2. Lesen und akzeptieren Sie die Lizenzbedingungen vor der Installation. Indem Sie den Parameter `-acceptLicense` der Befehlszeile hinzufügen, akzeptieren Sie alle Lizenzen.
3. Führen Sie den folgenden Befehl aus:

**Wichtig:** Wenn Sie Windows 7, Windows Vista oder Windows Server 2008 verwenden, starten Sie die Eingabeaufforderung, indem Sie mit der rechten Maustaste klicken und die Option **Als Administrator ausführen** auswählen.

Windows

```
extraktionsverzeichnis\IM\tools\imcl install liste_der_produk-IDs -acceptLicense -installationDirectory position -repos  
-properties schlüssel=wert,schlüssel=wert -showVerboseProgress -log protokollname.log
```

UNIX Linux

```
extraktionsverzeichnis/IM/tools/imcl install liste_der_produk-IDs -acceptLicense -installationDirectory position -repos  
-properties schlüssel=wert,schlüssel=wert -showVerboseProgress -log protokollname.log
```

Dabei gilt Folgendes:

- `liste_der_produk-IDs` ist eine durch Leerzeichen getrennte Liste aller IDs der Produkte, die Sie installieren möchten.

Tabelle 1. Produkt-IDs

Produkt	Produkt-ID	Feature	Beschreibung
IBM Business Monitor	com.ibm.websphere.MQ	IBM/Feature	Erforderlich. Laufzeitinhalt des IBM Business Monitor-Kerns.
		wbm.server.feature	Erforderlich. Laufzeitinhalt des IBM Business Monitor-Servers.
		wbm.profile.feature	Eigenständiges IBM Business Monitor-Entwicklungsprofil (qmwass).
		wbm.wps.profile.feature	Eigenständiges Entwicklungsprofil für IBM Business Monitor auf Process Server (qmbpmaps).
		wbm.esb.profile.feature	Eigenständiges Entwicklungsprofil für IBM Business Monitor auf WebSphere ESB (qmesb).

Tabelle 1. Produkt-IDs (Forts.)

Produkt	Produkt-ID	Feature	Beschreibung
WebSphere Application Server Network Deployment	com.ibm.websphere.ND.core	corefeature	Erforderlich. WebSphere Application Server-Kerninhalt.
		ejbdeploy	EJB-Module vor Enterprise JavaBeans 3.0.
		thinclient	Eigenständige Thin Clients und Ressourcenadapter.
		embeddablecontainer	Integrierbarer EJB-Container.
		Beispiele (samples)	Feature für Beispielanwendungen.
		com.ibm.sdk.6_32bit	32-Bit-Software-Development-Kit (SDK). Sie müssen entweder dieses Feature oder com.ibm.sdk.6_64bit angeben.
		com.ibm.sdk.6_64bit	64-Bit-Software-Development-Kit (SDK). Dieses Feature kann nur auf einem 64-Bit-System ausgewählt werden. Sie müssen entweder dieses Feature oder com.ibm.sdk.6_32bit angeben.
Installation Manager	com.ibm.cic.agent	Agentenkern (agent_core)	Installation Manager-Kerninhalt.
		agent_jre	Installation Manager Java Runtime Environment (JRE).
DB2 Express for Linux (32 Bit)	com.ibm.ws.DB2EXP97linuxia32	n/v	DB2 muss dem Betriebssystem und der Bitunterstützung entsprechen.
DB2 Express for Linux (64 Bit)	com.ibm.ws.DB2EXP97linuxia64	n/v	DB2 muss dem Betriebssystem und der Bitunterstützung entsprechen.
DB2 Express for Windows (32 Bit)	com.ibm.ws.DB2EXP97winia32	n/v	DB2 muss dem Betriebssystem und der Bitunterstützung entsprechen.
DB2 Express for Windows (64 Bit)	com.ibm.ws.DB2EXP97winia64	n/v	DB2 muss dem Betriebssystem und der Bitunterstützung entsprechen.



Tabelle 1. Produkt-IDs (Forts.)

Produkt	Produkt-ID	Feature	Beschreibung
IBM Cognos Business Intelligence for Windows x86 (32 Bit)	com.ibm.ws.cognos.v10h1/winia32		IBM Cognos BI muss dem Betriebssystem und der Bitunterstützung von WebSphere Application Server entsprechen.
IBM Cognos BI for Windows x64 (64 Bit)	com.ibm.ws.cognos.v10h1/winia64		IBM Cognos BI muss dem Betriebssystem und der Bitunterstützung von WebSphere Application Server entsprechen.
IBM Cognos BI for AIX PPC (32 Bit)	com.ibm.ws.cognos.v10h1/aix32		IBM Cognos BI muss dem Betriebssystem und der Bitunterstützung von WebSphere Application Server entsprechen.
IBM Cognos BI for AIX PPC (64 Bit)	com.ibm.ws.cognos.v10h1/aix64		IBM Cognos BI muss dem Betriebssystem und der Bitunterstützung von WebSphere Application Server entsprechen.
IBM Cognos BI for Linux x86 (32 Bit)	com.ibm.ws.cognos.v10h1/linuxia32		IBM Cognos BI muss dem Betriebssystem und der Bitunterstützung von WebSphere Application Server entsprechen.
IBM Cognos BI for Linux x86-64 (64 Bit)	com.ibm.ws.cognos.v10h1/linuxia64		IBM Cognos BI muss dem Betriebssystem und der Bitunterstützung von WebSphere Application Server entsprechen.
IBM Cognos BI for Solaris SPARC (32 Bit)	com.ibm.ws.cognos.v10h1/solaris32		IBM Cognos BI muss dem Betriebssystem und der Bitunterstützung von WebSphere Application Server entsprechen.

Tabelle 1. Produkt-IDs (Forts.)

Produkt	Produkt-ID	Feature	Beschreibung
IBM Cognos BI for Solaris SPARC (64 Bit)	com.ibm.ws.cognos.v10h1/solaris64		IBM Cognos BI muss dem Betriebssystem und der Bitunterstützung von WebSphere Application Server entsprechen.
IBM Cognos BI for Linux on System z	com.ibm.ws.cognos.v10h1/zlinux64		IBM Cognos BI muss dem Betriebssystem und der Bitunterstützung von WebSphere Application Server entsprechen.

- *position* ist der Pfad zu dem Verzeichnis, in dem Sie die Produkte installieren möchten.
- *repository* ist der Pfad zum Repository, wohin Sie die Dateien extrahiert haben, dies ist eines der folgenden Verzeichnisse:  
*extraktionsverzeichnis/repository/repos\_32bit*  
*extraktionsverzeichnis/repository/repos\_64bit*

Mehrere Repositories können Sie angeben, indem Sie die Repository-Positionen durch Kommas voneinander abgrenzen.

- *schlüssel=wert* ist eine Liste von Schlüsseln und Werten (durch Kommas getrennt), die Sie an die Installation übergeben wollen. Verwenden Sie vor und nach den Kommas keine Leerzeichen. Erstellen Sie mit IBM Installation Manager verschlüsselte Kennwörter.

Tabelle 2. Schlüssel

Schlüssel	Beschreibung
user.select.64bit.image	Wenn die Installation unter einem 64-Bit-Betriebssystem erfolgt, muss folgende Zeile genau wie hier angegeben hinzugefügt werden: <code>user.select.64bit.image,,com.ibm.websphere.ND.v80=true</code> Der Standardwert ist 'false'.
user.db2.admin.username	Nur unter Windows. Der Benutzername mit der Berechtigung auf die DB2-Datenbank zuzugreifen. Der Standardwert ist 'bpmadmin'.
user.db2.admin.password	Nur unter Windows. Das Kennwort für den oben angegebenen Benutzernamen. Wählen Sie ein Kennwort, das die Kennwortrichtlinie Ihres Systems (z. B. Windows 2008) einhält.
user.bpm.admin.username	Der Benutzername für die Administrationskonsole. Der Standardwert ist 'admin'. Diese Eigenschaft wird nur benötigt, wenn Sie gerade ein Profil erstellen.

Tabelle 2. Schlüssel (Forts.)

Schlüssel	Beschreibung
user.bpm.admin.password	Das Kennwort für den oben angegebenen Benutzernamen. Der Standardwert ist 'admin'. Diese Eigenschaft wird nur benötigt, wenn Sie gerade ein Profil erstellen.
user.db2.port	Der Port für die DB2-Datenbank. Der Standardwert ist '50000'.
user.db2.instance.username	Wird nur unter Linux verwendet. Der Benutzername der DB2-Instanz. Der Standardwert ist 'bpminst'.
user.db2.instance.password	Wird nur unter Linux verwendet. Das Kennwort für den oben angegebenen Benutzernamen.
user.db2.fenced.username	Wird nur unter Linux verwendet. Der Name des abgeschirmten Benutzers. Der Standardwert ist 'bpmfenc'.
user.db2.fenced.password	Wird nur unter Linux verwendet. Das Kennwort für den oben angegebenen Benutzernamen.
user.db2.das.username	Wird nur unter Linux verwendet. Der Benutzername des Verwaltungsservers (DAS). Der Standardwert ist 'bpadmin'.
user.db2.das.password	Wird nur unter Linux verwendet. Das Kennwort für den oben angegebenen Benutzernamen.

- *protokollname* ist der Name der Protokolldatei, in der Nachrichten und Ergebnisse aufgezeichnet werden.

Die Ausführung dieses Befehls installiert das Produkt mit seinen Standardmerkmalen. Wenn Sie bestimmte Komponenten (Features) installieren oder Änderungen vornehmen wollen, finden Sie entsprechende Informationen über den Referenzlink für Befehlszeilenargumente für den Befehl 'imcl'.

Installation Manager installiert diese Produktliste und schreibt eine Protokolldatei in das von Ihnen angegebene Verzeichnis.

Im folgenden Beispiel wird IBM Business Monitor unter Windows installiert.

```
imcl install com.ibm.websphere.MON.V80 com.ibm.websphere.ND.v80,core.feature,ejbdeploy,thinclient,
```

Sie müssen im Profile Management Tool oder mit dem Befehl 'manageprofiles' ein Profil für einen eigenständigen Server oder einen Deployment Manager definieren. In einer Produktionsumgebung können nur Profile verwendet werden, die mit dem Profile Management Tool oder dem Befehl 'manageprofiles' erstellt wurden.

## Unbeaufsichtigte Installation von IBM Business Monitor mithilfe einer Antwortdatei

Sie können IBM Business Monitor installieren, indem Sie zuerst eine Antwortdatei erstellen und dann einen entsprechenden Befehl ausführen, um das Produkt unter Verwendung dieser Antwortdatei zu installieren.

Vor der Installation von IBM Business Monitor sollten Sie die Systemanforderungen des Produkts prüfen.

Die vorausgesetzten Betriebssystem- und Softwareversionen sind besonders wichtig. Auch wenn der Installationsprozess automatisch eine Überprüfung auf vorausgesetzte Betriebssystemprogrammkorrekturen durchführt, sollten Sie die Systemanforderungen überprüfen (falls noch nicht geschehen). Der Link zu den Systemanforderungen listet alle unterstützten Betriebssysteme sowie die Fixes und Patches für die Betriebssysteme auf, die Sie installieren müssen, damit Ihr Betriebssystem kompatibel ist. Es werden auch die erforderlichen Versionen aller Softwarevoraussetzungen aufgeführt.

Wenn Sie planen, IBM Business Monitor unter Verwendung von DB2 Express unter Red Hat Enterprise Linux 6 zu installieren, stellen Sie sicher, dass der Benutzer über Administratorberechtigungen (Rootbenutzer) verfügt. Als Rootbenutzer müssen Sie außerdem sicherstellen, dass alle Kernelanforderungen erfüllt sind, bevor die Installation von DB2 Express beginnt. Sie können die aktuellen Werte lokalisieren, indem Sie die Ausgabe des Befehls `ipcs -l` analysieren.

Wenn Sie nicht über die für die Installation von IBM Business Monitor erforderlichen Basisprodukte verfügen, müssen Sie sie im Rahmen der unbeaufsichtigten Installation mitinstallieren. Folgende Basisprodukte sind erforderlich:

- Installation Manager
- WebSphere Application Server Network Deployment

Die unbeaufsichtigte Installation führt die folgenden Tasks aus:

- Installation von Installation Manager, falls das Produkt noch nicht installiert wurde, oder Aktualisierung des Produkts auf die geeignete Version, falls es bereits installiert ist.
- Die erforderlichen Basisprodukte sowie IBM Business Monitor werden installiert.

Gehen Sie wie folgt vor, um IBM Business Monitor im unbeaufsichtigten Modus zu installieren:

1. Führen Sie den folgenden Befehl aus, um mit IBM Installation Manager verschlüsselte Kennwörter zu generieren, damit sichere Verbindungen zu DB2 und zur WebSphere-Administrationskonsole hergestellt werden können.

**Wichtig:** Wenn Sie Windows 7, Windows Vista oder Windows Server 2008 verwenden, starten Sie die Eingabeaufforderung, indem Sie mit der rechten Maustaste klicken und die Option **Als Administrator ausführen** auswählen.

 Windows

```
IM-position\eclipse\tools\imutilsc -silent -nosplash encryptString zu_verschlüsselndes_kennwort
```

 Linux

```
IM-position/eclipse/tools/imutilsc -silent -nosplash encryptString zu_verschlüsselndes_kennwort
```


2. Lesen und akzeptieren Sie die Lizenzbedingungen vor der Installation. Indem Sie den Parameter `-acceptLicense` der Befehlszeile hinzufügen, akzeptieren Sie alle Lizenzen.
3. Erstellen Sie die Antwortdatei, mit deren Hilfe die erforderlichen Basisprodukte und IBM Business Monitor installiert werden. Kopieren Sie die Musterantwortdatei aus dem folgenden Verzeichnis, um eine eigene Antwortdatei zu erstellen:  
`extraktionsverzeichnis/responsefiles/WBM/template_response.xml`
4. Ändern Sie die Parameter, wie im Text in der Antwortdateischablone angegeben, um Ihre Antwortdatei zu erstellen. Sie können eine Antwortdatei auch erstellen, indem Sie Ihre Aktionen in Installation Manager aufzeichnen. Bei der Aufzeichnung einer Antwortdatei werden alle Einstellungen, die Sie in Installa-

tion Manager vornehmen, in einer XML-Datei gespeichert. Wenn Sie den Installation Manager im unbeaufsichtigten Modus ausführen, werden die Daten in der XML-Antwortdatei zur Ausführung der Installation verwendet.

**Wichtig:** Stellen Sie sicher, dass die Repository-Positionen am Anfang der Musterantwortdatei auf die korrekte Speicherposition in Ihrer Umgebung zeigen.

5. Führen Sie den folgenden Befehl aus:

**Wichtig:** Wenn Sie Windows 7, Windows Vista oder Windows Server 2008 verwenden, starten Sie die Eingabeaufforderung, indem Sie mit der rechten Maustaste klicken und die Option **Als Administrator ausführen** auswählen.

Benutzer mit Administrator-/Rootberechtigung: 

```
extraktionsverzeichnis\IM\installc.exe -acceptLicense input  
extraktionsverzeichnis\responsefiles\BusMon\template_response.xml -log bevorzugte_protokollpos
```

```
extraktionsverzeichnis/IM/installc -acceptLicense input  
extraktionsverzeichnis/responsefiles/BusMon/template_response.xml -log bevorzugte_protokollpos
```

Benutzer ohne Administrator-/Rootberechtigung: 

```
extraktionsverzeichnis\IM\userinstc.exe -acceptLicense input  
extraktionsverzeichnis\responsefiles\BusMon\template_response.xml -log bevorzugte_protokollpos
```

```
extraktionsverzeichnis/IM/userinstc -acceptLicense input  
extraktionsverzeichnis/responsefiles/BusMon/template_response.xml -log bevorzugte_protokollpos
```

Installation Manager installiert alle erforderlichen Voraussetzungen sowie IBM Business Monitor und schreibt eine Protokolldatei in das von Ihnen angegebene Verzeichnis.

Sie müssen im Profile Management Tool oder mit dem Befehl 'manageprofiles' ein eigenständiges Serverprofil oder einen Deployment Manager definieren. In einer Produktionsumgebung können nur Profile verwendet werden, die mit dem Profile Management Tool oder dem Befehl 'manageprofiles' erstellt wurden.

---

## Information Center installieren

Das Information Center für IBM Business Monitor ist über das Internet verfügbar. Sie können es aber auch über das Launchpad des Produkts installieren, sofern hierfür Unterstützung durch Ihr Betriebssystem gegeben ist.

- Installieren und starten Sie das Information Center über das Launchpad des Produkts.
  1. Klicken Sie im Launchpad auf **Help System installation** (Hilfesysteminstallation).
  2. Geben Sie einen Standort für das lokale Information Center an.
  3. Klicken Sie auf **Install and start the Help System** (Hilfesystem installieren und starten). Wenn das Fenster 'Open file' (Datei öffnen) angezeigt wird, klicken Sie auf **Ausführen**.
- Zeigen Sie das Information Center im Internet an. Informationen enthält IBM Business Process Management Information Center.

## Lokales Information Center starten und stoppen

Nach der Installation des IBM Business Monitor Information Centers können Sie das Information Center auf Ihrem lokalen System wie im Folgenden angegeben anzeigen oder im Netz für andere Benutzer bereitstellen.


Hierbei steht `doc_root` für das Verzeichnis, in dem das Information Center installiert werden soll.

- Führen Sie die folgenden Schritte aus, um das Information Center lokal anzuzeigen:
  1. Wechseln Sie in das Verzeichnis, in dem das Information Center installiert ist.
  2. Wenn Sie das Information Center starten möchten, führen Sie das für Ihr Betriebssystem vorgesehene Script aus:
    - `help_start.sh`
    - `help_start.bat`Ihr Standardbrowser wird geöffnet und zeigt das mit dem Produkt installierte Information Center an.
  3. Wenn Sie das Information Center stoppen möchten, schließen Sie den Browser und führen Sie das für Ihr Betriebssystem vorgesehene Script aus:
    - `help_end.sh`
    - `help_end.bat`
- Führen Sie die folgenden Schritte aus, wenn Sie das Information Center auf einem Host bereitstellen möchten, um die Informationen auf anderen Systemen im Netz anzuzeigen:
  1. Wechseln Sie in das Verzeichnis, in dem IBM Business Monitor installiert ist.
  2. Wenn Sie das Information Center starten möchten, führen Sie das für Ihr Betriebssystem vorgesehene Script aus:
    - `IC_start.sh`
    - `IC_start.bat`Benutzer, die sich an anderen Systemen im Netz befinden, können an diesen Systemen einen Browser öffnen und das Information Center über folgende URL aufrufen:  
`http://hostname:8888/help/index.jsp`
  3. Wenn Sie das Information Center stoppen möchten, schließen Sie den Browser und führen Sie das für Ihr Betriebssystem vorgesehene Script aus:
    - `IC_end.sh`
    - `IC_end.bat`

## Lokales Information Center aktualisieren

Wenn Sie über eine Internetverbindung verfügen, kann Ihre lokal installierte Version der Dokumentation aktualisiert werden, wenn neue Dokumentation verfügbar ist. Möglicherweise gibt es auch für andere Produkte aktualisierte Dokumentationen, die Sie in das lokale Information Center übernehmen können.

Gehen Sie wie folgt vor, um die Dokumentation zu aktualisieren:

1. Klicken Sie in der Symbolleiste des Hilfesystems auf das Symbol **Aktualisieren**.  
() Es wird eine Liste mit allen Dokumentationssätzen, die bereits installiert sind, angezeigt.
2. Klicken Sie am Ende der Liste mit der installierten Dokumentation auf **Weiter**. Es wird eine Liste mit installierbaren Dokumentationssätzen angezeigt. Diese

Sätze enthalten Produktdokumentationen in verschiedenen Sprachen und können auch Dokumentationsätze für andere Produkte enthalten.

3. Wählen Sie die Dokumentation aus, die Sie installieren möchten.

**Tipp:** Sie können mehrere Dokumentationsätze auswählen.

Die Dokumentation für das ausgewählte Produkt bzw. die ausgewählten Produkte wird im Hilfesystem Ihres Computers installiert.





---

## Kapitel 5. Datenbanken erstellen

Für IBM Business Monitor sind zwei Datenbanken erforderlich, wobei eine für die IBM Business Monitor-Konfiguration und eine für den IBM Cognos Business Intelligence-Content-Store verwendet wird.

### Monitor- und COGNOSCS-Datenbank

Standardmäßig heißt die Datenbank für IBM Business Monitor MONITOR und die Datenbank für den IBM Cognos BI-Content-Store heißt COGNOSCS.

Sie können die Datenbanken MONITOR und COGNOSCS bei der Erstellung eines eigenständigen Profils oder eines Deployment Manager-Profiles erstellen, Sie können das Datenbankentwurfstool (dbDesignGenerator) verwenden oder Sie können die Datenbanken manuell erstellen, indem Sie die Datenbanksriptdateien vor oder nach der Profilerstellung ausführen. In einer Network Deployment-Umgebung ist es am besten, die Datenbanken vor dem Start von Deployment Manager und der Erstellung weiterer angepasster Profile zu erstellen.

**Wichtig:** Wenn Sie DB2 for z/OS verwenden, erstellen Sie die Datenbank mit dem Datenbankentwurfstool (dbDesignGenerator) oder stellen Sie die Datenbank manuell.

Wenn Sie über einen IBM Cognos BI-Server verfügen, dann müssen Sie keine COGNOSCS-Datenbank erstellen, weil der Content-Store bereits definiert wurde.

**Tipp:** Wenn sich die COGNOSCS-Datenbank nicht lokal auf dem IBM Cognos BI-Server befindet, müssen Sie einen Datenbankclient auf der IBM Cognos BI-Servermaschine installieren. Details hierzu enthalten die entsprechenden Abschnitte mit datenbankspezifischen Datenbankhinweisen.

Die MONITOR- und die COGNOSCS-Datenbank dürfen sich auf demselben Server, auf dem sich der IBM Business Monitor-Server befindet, oder auf einem anderen Server befinden. Um die Datenbanken für die Profilerstellung automatisch zu erstellen, muss Ihr Datenbankserver sich lokal auf dem System befinden, auf dem Sie das Profile Management Tool oder den Befehl **manageprofiles** ausführen. Andernfalls verwenden Sie die Datenbanksriptdateien zur Erstellung der Datenbanken. Verwenden Sie die Datenbanksriptdateien auch dann zur Erstellung der Datenbanken, wenn Sie z/OS verwenden, oder wenn der Datenbankserver mehrere Versionen der Datenbank oder mehrere Datenbankinstanzen enthält.

### Datenbankskripts

Wenn Sie ein eigenständiges oder ein Deployment Manager-Profil erstellen, werden Datenbankskripts generiert, die mit den während der Profilerstellung eingegebenen Werten übereinstimmen. Auf diese Weise wird sichergestellt, dass die Namen auf dem IBM Business Monitor-Server und in der IBM Business Monitor-Datenbank konsistent sind.

Sie können die Datenbankskripts auch selbst erstellen, indem Sie eine der folgenden Methoden anwenden:

- Konfigurieren Sie die Werte mithilfe des Datenbankentwurfstools (DbDesignGenerator), das mit dem IBM Business Monitor-Server installiert wird. Ein Vorteil

der Verwendung des Datenbankentwurfstools liegt darin, dass Sie die Monitor-Datenbank, die IBM Cognos BI-Datenbank, die Business Space-Datenbank und die Datenbanken für die Messaging-Steuerkomponenten für IBM Business Monitor und die CEI (Common Event Infrastructure) alle gleichzeitig entwerfen können. Anweisungen finden Sie unter „Datenbankscrippts mit dem Datenbankentwurfstool erstellen oder konfigurieren“ auf Seite 61.

- Konfigurieren Sie die Werte manuell. Anweisungen finden Sie unter „MONITOR-Datenbankscrippts manuell konfigurieren“ auf Seite 62.

Nach der Generierung oder Anpassung der Datenbankscrippts führen Sie die Scrippts wie in „Monitor-Datenbank manuell installieren“ auf Seite 67 beschrieben aus.

## **Tabellen der Messaging-Steuerkomponenten**

Die Messaging-Steuerkomponenten für den IBM Business Monitor-Service Integration Bus und den CEI-Bus (CEI = Common Event Infrastructure) benötigen Datenbanktabellen. Außer auf z/OS können diese Tabellen automatisch von WebSphere Application Server erstellt werden, wenn der Datenbankbenutzer von IBM Business Monitor über ausreichende Berechtigungen verfügt und die Option zum automatischen Erstellen von Tabellen bei den Nachrichtenspeicheroptionen des Service Integration Bus ausgewählt ist. Diese Option wird standardmäßig auf 'true' gesetzt, es sei denn, Sie verwenden DB2 for z/OS.

Die Datenbankscrippts für die Tabellen der Messaging-Steuerkomponente können ebenfalls mithilfe einer der folgenden Optionen generiert werden:

- Erstellen Sie das Script mithilfe des Datenbankentwurfstools (DbDesignGenerator). Anweisungen finden Sie unter „Datenbankscrippts mit dem Datenbankentwurfstool erstellen oder konfigurieren“ auf Seite 61.
- Erstellen Sie die Tabellen manuell. Anweisungen finden Sie unter „Tabellen für Messaging-Steuerkomponente manuell erstellen“ auf Seite 70.

## **Business Space-Tabellen**

Wenn Sie Business Space verwenden, müssen Sie auch die Business Space-Tabellen konfigurieren, wobei Sie entweder die Scrippts, die während der Erstellung des eigenständigen Profils generiert wurden, oder das Datenbankentwurfstool verwenden. Weitere Informationen finden Sie in Business Space-Datenbanktabellen konfigurieren im Business Space Information Center.

## **Datenbanksicherheit**

Wenn die Datenbanken erstellt werden, werden dem Benutzer der Laufzeitdatenbank standardmäßig Berechtigungen zur Verwaltung von Datenbankobjekten erteilt. Dies vereinfacht die Erstellung von Datenbanken und ermöglicht dem IBM Business Monitor-Server, das Datenbankschema des Monitor-Modells automatisch bei der Implementierung und Entfernung der Modelle zu verwalten. Wenn die Datenbanken geschützt werden müssen, finden Sie weitere Informationen in den Abschnitten Monitor-Datenbankumgebung schützen und IBM Cognos BI-Sicherheit konfigurieren.

---

## Datenbankscripits mit dem Datenbankentwurfstool erstellen oder konfigurieren

Das Datenbankentwurfstool (DbDesignGenerator), das mit dem IBM Business Monitor-Server installiert wird, kann zum Generieren von Datenbankscripits verwendet werden, die vor oder nach der IBM Business Monitor-Profilerstellung ausgeführt werden können.

Ein Vorteil der Verwendung des Datenbankentwurfstools besteht darin, dass Sie die Datenbanken gleichzeitig für IBM Business Monitor, IBM Cognos BI, Business Space und für die Messaging-Steuerkomponente entwerfen können. Datenbankscripits werden für jede Komponente generiert. Ferner wird eine 'dbdesign'-Datei generiert, die später an den Implementierungsumgebungsassistenten übergeben werden kann, um die Datenquellen bei der Erstellung einer komplexen IBM Business Monitor-Topologie automatisch zu konfigurieren.

**Wichtig:** Stellen Sie sicher, dass Sie das Datenbankentwurfstool verwenden, wenn Sie Datenbanken für DB2 for z/OS erstellen.

Wenn Sie den Pfad **Erweitert** über das Profile Management Tool auswählen, dann können Sie **Datenbank mit einer Entwurfsdatei konfigurieren** auswählen und eine Entwurfsdatei auswählen, die Sie bereits erstellt haben.

Weitere Informationen zum Datenbankentwurfstool finden Sie in den zugehörigen Links.

Führen Sie folgende Schritte aus, um die Datenbankscripdateien mit dem Datenbankentwurfstool zu bearbeiten:

1. Wechseln Sie in das Verzeichnis `application_server-stammverzeichnis/util/dbUtils`.
2. Führen Sie den Befehl aus, um das Dienstprogramm zu starten.
  - `DbDesignGenerator.bat`
  - `DbDesignGenerator.sh`
3. Wählen Sie im Hauptmenü die Option **(1) Create a database design for Standalone profile or Deployment Environment** (1 - Datenbankentwurf für eigenständiges Profil oder Implementierungsumgebung erstellen) aus.
4. Wählen Sie in der Eingabeaufforderung **Please pick one of the following db designs that are supported** (Wählen Sie eines der folgenden unterstützten Datenbankdesigns) die Option **(1)monitor.nd.topology** oder die Option **(2)monitor.standalone** aus. Die Option 'monitor.nd.topology' bietet mehr Flexibilität bei der Verteilung der Datenbankkomponenten über mehrere Datenbanken.
5. Wählen Sie an der Eingabeaufforderung **Please pick one of the following [database component(s)]** (Wählen Sie eine der folgenden [Datenbankkomponente(n)]) die Option **(1)[Monitor] MONITOR : [master] [status = not complete]** aus.
6. Geben Sie in der Eingabeaufforderung **Edit this db component?** (Diese Datenbankkomponente bearbeiten?) `y` (ja) ein.
7. Wählen Sie in der Eingabeaufforderung **Please pick one of the following DB types that are supported** (Wählen Sie einen der folgenden unterstützten Datenbanktypen) die Nummer Ihrer Datenbankplattform aus.
8. Beantworten Sie die Eingabeaufforderungen der Reihe nach oder drücken Sie gegebenenfalls die Eingabetaste, um die Standardwerte zu akzeptieren. Sie

werden dazu aufgefordert, Datenbanknamen, Schemanamen, Benutzernamen und Kennwort sowie das Verzeichnispräfix des Tabellenbereichs einzugeben.

9. Geben Sie in der Eingabeaufforderung **To skip data source properties, enter 's'; or enter anything else to continue** (Geben Sie zum Überspringen der Datenquelleneigenschaften 's' ein oder geben Sie einen anderen Buchstaben ein, um fortzufahren) den Buchstaben **c** (oder ein beliebiges anderes Zeichen außer **s**) ein, um mit der Eingabe der Informationen fortzufahren.
10. Beantworten Sie die Eingabeaufforderungen der Reihe nach oder drücken Sie gegebenenfalls die Eingabetaste, um die Standardwerte zu akzeptieren. Sie werden aufgefordert, die Eigenschaften für Ihre Datenquelle einzugeben.
11. Stellen Sie sicher, dass die IBM Business Monitor-Datenbankkomponente vollständig ist, bevor Sie mit der Konfiguration der übrigen Komponenten fortfahren. Die IBM Cognos BI-Datenbank wird als nicht vollständig angezeigt und erfordert die Angabe eines Datenbankbenutzers mit dem zugehörigen Kennwort. Für die übrigen Einstellungen können Sie die Standardwerte übernehmen.
12. Wenn die Eingabeaufforderung **Please pick one of the following [database component(s)]** (Wählen Sie eine der folgenden [Datenbankkomponenten]) erneut angezeigt wird, dann ist die Eingabe der Eigenschaften abgeschlossen, wenn in allen Zeilen **[status = complete]** angezeigt wird, z. B. **(1)[Monitor] MONITOR : [master] [status = complete]**. Geben Sie **5 [save and exit]** ein und drücken Sie die Eingabetaste, um den Datenbankentwurf zu speichern. Nach Abschluss der MONITOR-Konfiguration müssen zusätzliche Konfigurationsschritte für die Datenbankkomponente **[Cognos] COGNOSCS** ausgeführt werden. Der COGNOSCS-Status lautet so lange **[status = not complete]**, bis diese Komponente vollständig konfiguriert worden ist.
13. Drücken Sie in der Eingabeaufforderung **Please enter the output directory** (Ausgabeverzeichnis eingeben) die Eingabetaste, um den Standardwert zu akzeptieren (`application_server-stammverzeichnis/util/dbUtils`) oder geben Sie den Standort ein, um die Datenbankentwurfsdateien zu schreiben.
14. Drücken Sie in der Eingabeaufforderung **Please enter the output filename** (Namen der Ausgabedatei eingeben) die Eingabetaste, um den Standardwert zu akzeptieren (`monitor.standalone.dbdesign`) oder geben Sie einen Namen für die Datei ein.
15. Geben Sie in der Eingabeaufforderung **Generate db script?** (Datenbanksript generieren?) **y** (ja) ein und drücken Sie die Eingabetaste wiederholt, um die Standardpositionen zu akzeptieren. Für die Monitor- und COGNOSCS-Datenbanksripts, das Datenspeichersript der Messaging-Steuerkomponente und für die Business Space-Datenbanksripts werden Unterverzeichnisse erstellt.

---

## MONITOR-Datenbanksripts manuell konfigurieren

Die Datenbanksripts, die für die Erstellung der MONITOR-Datenbank erforderlich sind, werden auf den Installationsmedien ausgeliefert und während der Installation des IBM Business Monitor-Servers auf den Anwendungsserver kopiert. Diese Datenbanksripts können manuell angepasst werden, sodass Sie die Datenbanken vor der Serverinstallation oder der Profilerstellung erstellen können.

Führen Sie folgende Schritte aus, um die Datenbanksripts manuell zu bearbeiten:

1. Öffnen Sie die Datenbanksriptdateien für Ihre Datenbanksoftware mit einem Texteditor.

Die Scripts erstellen die Datenbanken und die erforderlichen Tabellen für IBM Business Monitor.

- **Für DB2 for z/OS:**
  - createDatabase\_Monitor.sql
  - createTablespace\_Monitor.sql
  - createTable\_Monitor.sql
- **Für alle anderen Datenbanken:**
  - createDatabase.sql
  - createTables.sql

Die Dateien befinden sich standardmäßig in den folgenden Verzeichnissen:

(nur dezentral) *DVD\_stammverzeichnis/scripts/database/Monitor/plattform*  
*application\_server-stammverzeichnis/dbscripts/Monitor*  
*application\_server-stammverzeichnis/profiles/profilname/dbscripts/*  
*Monitor* (eigenständig)

*application\_server-stammverzeichnis/profiles/profilname/*  
*dbscripts.wbm* (Deployment Manager)

Hierbei gilt Folgendes:

*DVD\_stammverzeichnis* ist das Verzeichnis, in das Sie das CD-Image bzw. das für den Download verfügbare Image extrahiert haben.

*plattform* ist das Betriebssystem der Datenbank (beispielsweise DB2, Oracle oder SQL Server).

*stammverzeichnis\_des\_anwendungsservers* ist das Verzeichnis, in dem IBM Business Monitor installiert ist.

2. Bearbeiten Sie die folgenden Variablen in den Datenbankscripdateien für Ihre Datenbanksoftware:

- **Bearbeiten Sie für DB2** die folgenden Variablen:

**@DB\_NAME@**

Stellt den Namen der IBM Business Monitor-Datenbank dar (Beispiel: MONITOR).

**@SCHEMA@**

Stellt den Namen des IBM Business Monitor-Schemas dar (Beispiel: MONITOR).

**@TSDIR@**

Stellt das Tabellenbereichsverzeichnis dar.

Wenn @TSDIR@ in der Datendateispezifikation eines Tabellenbereichs nicht angegeben wird, wird die Datendatei im Verzeichnis des Datenbankmanagers erstellt.

**@DB\_USER@**

Stellt den Laufzeitbenutzer der IBM Business Monitor-Datenbank dar.

- **Bearbeiten Sie für DB2 for z/OS** die folgenden Variablen:

**@STOGRP@**

Stellt den DB2-Speichergruppennamen dar (Beispiel: SYSDEFLT).

**@DB\_NAME@**

Stellt den Namen der IBM Business Monitor-Datenbank dar.

**@SCHEMA@**

Stellt den Namen des Qualifikationsmerkmals für das IBM Business Monitor-Schema dar.

**@DB\_USER@**

Stellt den Laufzeitbenutzer der IBM Business Monitor-Datenbank dar.

- **Bearbeiten Sie für SQL Server** die folgenden Variablen:

**@DB\_NAME@**

Stellt den Namen der IBM Business Monitor-Datenbank dar (Beispiel: MONITOR).

**@SCHEMA@**

Stellt den Namen des IBM Business Monitor-Schemas dar (Beispiel: MONITOR).

**@DB\_USER@**

Stellt den Laufzeitbenutzer der IBM Business Monitor-Datenbank dar.

**@DB\_PASSWORD@**

Stellt das Kennwort des IBM Business Monitor-Laufzeitdatenbankbenutzers dar. Sie können den Datenbankbenutzer und das zugehörige Kennwort vor der Ausführung des Scripts erstellen oder das Script so gestalten, dass es Datenbankbenutzer und Kennwort für Sie erstellt. Wenn das Script den Datenbankbenutzer und das Kennwort erstellen soll, müssen Sie @DB\_PASSWORD@ im Script angeben.

- **Bearbeiten Sie für Oracle** die folgenden Variablen:

**@SCHEMA@**

Stellt den Namen des Datenbankbenutzers dar, der Eigner der IBM Business Monitor-Datenbanktabellen ist.

**@DB\_PASSWORD@**

Stellt das Kennwort für den Datenbankbenutzer dar, der durch \$SCHEMA\$ angegeben wird.

**@TSDIR@**

Stellt das Tabellenbereichsverzeichnis dar.

Wenn @TSDIR@ in der Datendateispezifikation eines Tabellenbereichs nicht angegeben wird, wird die Datendatei im Verzeichnis des Datenbankmanagers erstellt. Wenn für @TSDIR@ ein vollständig qualifizierter Pfad angegeben wird, muss das Verzeichnis vorhanden sein, bevor dieses Script aufgerufen wird.

**@DB\_USER@**

Stellt den Laufzeitbenutzer der IBM Business Monitor-Datenbank dar.

Die Tabellenbereiche werden in der Datei createDatabase.sql erstellt. Wenn Sie die standardmäßig definierten Tabellenbereichsnamen durch eigene Tabellenbereichsnamen ersetzen, müssen Sie die Modellschemascripts bei der Implementierung der Modelle exportieren und so ändern, dass sie sich auf die ausgewählten Tabellenbereichsnamen beziehen.

**Wichtig:** Wenn Sie eine zusätzliche Monitoring-Instanz innerhalb derselben Oracle-Installation konfigurieren, müssen Sie darüber hinaus die Zeichenfolge DEFAULTTS in der Datei 'createDatabase.sql' in den folgenden vier Zeilen durch eine eindeutige Kennung für diese zusätzliche Monitoring-Instanz ersetzen:



```

CREATE TABLESPACE MONDSTS
  DATAFILE 'DEFAULTTS_MONDSTS.dbf' SIZE 500M AUTOEXTEND ON
NEXT 100M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONDMSTS
  DATAFILE 'DEFAULTTS_MONDMSTS.dbf' SIZE 100M AUTOEXTEND ON
NEXT 20M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONIDXTS
  DATAFILE 'DEFAULTTS_MONIDXTS.dbf' SIZE 250M AUTOEXTEND ON
NEXT 50M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONLOBTS
  DATAFILE 'DEFAULTTS_MONLOBTS.dbf' SIZE 200M AUTOEXTEND ON
NEXT 40M MAXSIZE UNLIMITED LOGGING; ;

```

Lautet die eindeutige Kennung für die zusätzliche Monitoring-Instanz z. B. MONDEV1\_MONDSTS, müssen die bearbeiteten Zeilen wie folgt aussehen:

```

CREATE TABLESPACE MONDSTS
  DATAFILE 'MONDEV1_MONDSTS.dbf' SIZE 500M AUTOEXTEND ON
NEXT 100M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONDMSTS
  DATAFILE 'MONDEV1_MONDMSTS.dbf' SIZE 100M AUTOEXTEND ON
NEXT 20M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONIDXTS
  DATAFILE 'MONDEV1_MONIDXTS.dbf' SIZE 250M AUTOEXTEND ON
NEXT 50M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONLOBTS
  DATAFILE 'MONDEV1_MONLOBTS.dbf' SIZE 200M AUTOEXTEND ON
NEXT 40M MAXSIZE UNLIMITED LOGGING;

```

Wiederholen Sie diese Schritte für jede einzelne zusätzliche Monitoring-Instanz.

**Anmerkung:** In Version 6.2 von IBM Business Monitor wurden andere Tabellenbereiche als in den vorherigen Versionen verwendet. Wählen Sie eine der folgenden Optionen, wenn Sie Oracle verwenden und ein Modell aus Version 6.1 in IBM Business Monitor 8.0 implementieren möchten:

- Führen Sie die Tabellenbereichsanweisungen aus Version 6.1 während der Installation der 8.0-Datenbank aus.
- Exportieren Sie das Modelldatenbanksript und ändern Sie die Tabellenbereichsreferenzen manuell so, dass Sie auf die Tabellenbereichsnamen der Version 7.0 zeigen, wenn Sie ein Monitormodell implementieren. Wenn Sie sich für die zweite Option entscheiden, müssen Sie diesen Vorgang immer dann ausführen, wenn Sie ein Modell der Version 6.1 auf einem Server der Version 7.0 implementieren.

Eine einfache Methode zur Vermeidung dieses Problems ist es, mit den bestehenden implementierten Modellen von Version 6.1 auf 8.0 zu migrieren und dann neue Modelle im Entwicklungstoolkit von Version 6.2 oder von 8.0 IBM Business Monitor zu generieren.

Die nachfolgende Tabelle enthält die Zuordnung der Tabellenbereichsnamen.

*Tabelle 3. Zuordnung der Tabellenbereichsnamen aus früheren IBM Business Monitor-Versionen*

Aktueller Tabellenbereich	Tabellenbereich der Version 6.1.x
MONDSTS	INSTANCE

Tabelle 3. Zuordnung der Tabellenbereichsnamen aus früheren IBM Business Monitor-Versionen (Forts.)

Aktueller Tabellenbereich	Tabellenbereich der Version 6.1.x
MONDMSTS	DMSTS
MONIDXTS	INDEXTS
MONLOBTS	LOBTS

3. Speichern und schließen Sie die Datei.

## COGNOSCS-Datenbankskripts manuell konfigurieren

Die für die Erstellung der COGNOSCS-Datenbank für IBM Cognos Business Intelligence erforderlichen Datenbankskripts werden auf den Installationsmedien mitgeliefert und während der Serverinstallation von IBM Business Monitor auf den Anwendungsserver kopiert. Diese Datenbankskripts können manuell angepasst werden, sodass Sie die Datenbanken vor der Serverinstallation oder der Profilerstellung erstellen können.

Führen Sie folgende Schritte aus, um die Datenbankskripts manuell zu bearbeiten:

- Öffnen Sie die Datenbanksriptdatei für Ihre Datenbanksoftware mit einem Texteditor.
  - Für DB2 for z/OS erstellt das Script `createDatabase_Cognos.sql` die Datenbank.
  - Für alle anderen Datenbanken erstellt das Script `createDatabase.sql` die Datenbank.

Die Datei befindet sich standardmäßig in den folgenden Verzeichnissen:

```
application_server-stammverzeichnis/dbscripts/Cognos
application_server-stammverzeichnis/profiles/profilname/dbscripts/
Cognos
```

Hierbei gilt Folgendes:

*stammverzeichnis\_des\_anwendungsservers* ist das Verzeichnis, in dem IBM Business Monitor installiert ist.

- Bearbeiten Sie die folgenden Variablen in den Datenbanksriptdateien für Ihre Datenbanksoftware:
  - Bei DB2 for z/OS** wird das Standardschema für den Datenbankbenutzer verwendet. Bearbeiten Sie folgende Variablen:

**@STOGRP@**  
Stellt den DB2-Speichergruppennamen dar (Beispiel: SYSDEFLT).

**@COG\_DB\_NAME@**  
Stellt den Namen der IBM Business Monitor-Datenbank dar (Beispiel: COGNOSCS).
  - Bei allen anderen Datenbanken** wird das Standardschema und der Standardtabellenbereich für den Datenbankbenutzer verwendet. Bearbeiten Sie folgende Variablen:

**@COG\_DB\_NAME@**  
Stellt den Namen der IBM Business Monitor-Datenbank dar (Beispiel: COGNOSCS).

**@DB\_USER@**  
Stellt den Laufzeitbenutzer der IBM Business Monitor-Datenbank dar.



3. Speichern und schließen Sie die Datei.
4. **Nur bei DB2 for z/OS:**
  - a. In DB2 for z/OS müssen Sie Tabellenbereiche mithilfe der IBM Cognos BI-Scripts `tablespace_db2z0S.sql` und `NC_TABLESPACES.sql` erstellen. Die vollständige Anleitung hierzu finden Sie im Information Center für IBM Cognos BI:
 

Vorgeschlagene Einstellungen für die Erstellung des Content-Store in DB2 unter z/OS

Tabellebereiche für einen DB2-Content-Store unter z/OS erstellen
  - b. Wenn IBM Cognos BI zum ersten Mal startet, erstellt es die Tabellen mithilfe folgender Scripts:
 

```
COGNOS_speicherposition/configuration/schemas/content/db2z0S/dbInitTest_db2z0S.sql
COGNOS_speicherposition/configuration/schemas/content/db2z0S/dbInitScript_db2z0S.sql
COGNOS_speicherposition/configuration/schemas/content/db2z0S/dbInitLock_db2z0S.sql
COGNOS_speicherposition/configuration/schemas/content/db2z0S/dbInitMeta_db2z0S.sql
COGNOS_speicherposition/configuration/schemas/delivery/zosdb2/NC_CREATE_DB2.sql
```

In Network Deployment-Umgebungen (ND) werden diese Dateien beim ersten Serverstart aus dem Master-Installationsverzeichnis für IBM Cognos BI in das entsprechende Serververzeichnis kopiert. Stellen Sie sicher, dass Sie die umgebungsspezifischen Variablen in diesen Dateien entsprechend ersetzt haben, bevor der IBM Cognos BI-Server startet; sonst verursachen die Tabellenerstellungsscripts Fehler, wenn der Server startet. Zur Bestimmung Ihrer `COGNOS_speicherposition` siehe Ihr IBM Cognos BI-Stammverzeichnis zur Laufzeit suchen.

---

## Monitor-Datenbank manuell installieren

Sie können die Datenbankskripts verwenden, um die IBM Business Monitor-Datenbank manuell entweder auf demselben Server wie den IBM Business Monitor-Server oder als ferne Datenbank auf einem anderen Server zu installieren. Stellen Sie vor der Ausführung der Scripts sicher, dass die umgebungsspezifischen Variablen in den Scripts entweder manuell oder mithilfe des Datenbankentwurfstools konfiguriert wurden.

Bevor Sie diese Task ausführen, stellen Sie bitte sicher, dass Sie den Abschnitt 'Hinweise zur Datenbankplanung' gelesen und alle Voraussetzungen für Ihr spezifisches Datenbankprodukt erfüllt haben. Wenn Sie zum Beispiel DB2 for z/OS verwenden, wird eine dedizierter Speichergruppe (STOGROUP) für IBM Business Monitor empfohlen. Die Speichergruppe muss erstellt werden, bevor die Datenbank erstellt wird.

Führen Sie auf dem Server, auf dem die Datenbanksoftware installiert ist, die folgenden Schritte aus:

1. Melden Sie sich beim Datenbankserver als Benutzer mit der Berechtigung zum Erstellen von Tabellenbereichen und Datenbankobjekten an.
2. Suchen Sie die DDL-Skripts.

- Wenn Sie die Scripts verwenden, die bei der Installation von IBM Business Monitor bereitgestellt werden, befinden sich diese im Verzeichnis `application_server-stammverzeichnis/dbscripts/Monitor`.
  - Wenn Sie die Scripts mit ersetzten Variablenwerten mithilfe des Befehls 'DbDesignGenerator' generiert haben, finden Sie sie in dem Ausgabeverzeichnis (standardmäßig `application_server-stammverzeichnis/util/dbUtils`), das Sie bei der Ausführung des Dienstprogramms ausgewählt haben.
  - Wenn Sie die Scripts mit ersetzten Variablenwerten mithilfe der Profilerstellung generiert haben, befinden sie sich in dem Ausgabeverzeichnis (standardmäßig `application_server-stammverzeichnis/profiles/<profil>/dbscripts/Monitor`), das Sie bei der Erstellung des Profils ausgewählt haben.
3. Führen Sie in der Befehlszeilenschnittstelle das Script durch den folgenden Befehl für Ihre Datenbanksoftware aus. Das Script erstellt die Datenbank für IBM Business Monitor.

- **DB2:** `db2 -tf createDatabase.sql`
- **DB2 for z/OS:**
  - `db2 -tf createDatabase_Monitor.sql`
  - `db2 -tf createTablespace_Monitor.sql`

Die Datenbankskripts können mit einem der Dienstprogramme SPUFI oder DSNTEP2 ausgeführt werden.

- **Oracle:** `sqlplus dbadmin/kennwort @ datenbankname @createDatabase.sql`. Dabei gilt:
  - dbadmin* ist ein Oracle-Benutzer mit Administratorberechtigung.
  - datenbankname* ist die Oracle-ID (z. B. orcl).
- **Microsoft SQL Server:** `sqlcmd -U dbadmin -P kennwort -e -i createDatabase.sql`. Dabei gilt:
  - dbadmin* ist ein SQL Server-Benutzer mit Administratorberechtigung.

4. Führen Sie das Script zum Erstellen von Tabellen mit einem der folgenden Befehle aus:

- **DB2:**
  - `db2 connect to MONITOR`
  - `db2 -tf createTables.sql`
  - `db2 connect reset`

**Anmerkung:** Während der Ausführung der DDL-Datei kann folgender Warnhinweis angezeigt werden: `SQL0347W The recursive common table expression "MON023.WBITIME" may contain an infinite loop. SQLSTATE=01605.` (`SQL0347W Der rekursive allgemeine Tabellenausdruck "MON023.WBITIME" kann eine Endlosschleife enthalten. SQLSTATE=01605`). Sie können diese Nachricht ignorieren.

- **DB2 for z/OS :**
  - `db2 connect to MONITOR`
  - `db2 -tf createTable_Monitor.sql`
  - `db2 connect reset`

**Anmerkung:** Während der Ausführung der DDL-Datei kann folgender Warnhinweis angezeigt werden: `SQL0347W The recursive common table expression "MON023.WBITIME" may contain an infinite loop. SQLSTATE=01605.` (`SQL0347W Der rekursive allgemeine Tabellenausdruck "MON023.WBITIME" kann eine Endlosschleife enthalten. SQLSTATE=01605`). Sie können diese Nachricht ignorieren.

- **Oracle:** `sqlplus benutzer/kennwort@datenbankname @createTables.sql`

- **Microsoft SQL Server:** `sqlcmd -U benutzer -P kennwort -e -i createTables.sql`
5. Starten Sie WebSphere Application Server.

---

## COGNOSCS-Datenbank manuell installieren

Mit dem Script `createDatabase` bzw. für DB2 for z/OS mit dem Script `createDatabase_Cognos` können Sie die Datenbank für den IBM Cognos Business Intelligence-Content-Store manuell entweder auf dem selben Server wie den IBM Business Monitor-Server oder als ferne Datenbank auf einem anderen Server installieren. Stellen Sie vor der Ausführung des Scripts sicher, dass die umgebungsspezifischen Variablen in dem Script entweder manuell oder mithilfe des Datenbankentwurfstools konfiguriert wurden.

Bevor Sie diese Task ausführen, stellen Sie bitte sicher, dass Sie den Abschnitt 'Hinweise zur Datenbankplanung' gelesen und alle Voraussetzungen für Ihr spezifisches Datenbankprodukt erfüllt haben.

Führen Sie auf dem Server, auf dem die Datenbanksoftware installiert ist, die folgenden Schritte aus:

1. Melden Sie sich beim Datenbankserver als Benutzer mit der Berechtigung zum Erstellen von Tabellenbereichen und Datenbankobjekten an.
2. Suchen Sie die DDL-Scripts.
  - Wenn Sie die Scripts verwenden, die bei der Installation von IBM Business Monitor bereitgestellt werden, befinden sich diese im Verzeichnis `application_server-stammverzeichnis/dbscripts/Cognos`.
  - Wenn Sie die Scripts mit ersetzten Variablenwerten mithilfe des Befehls 'DbDesignGenerator' generiert haben, finden Sie sie in dem Ausgabeverzeichnis (standardmäßig `application_server-stammverzeichnis/util/dbUtils`), das Sie bei der Ausführung des Dienstprogramms ausgewählt haben.
  - Wenn Sie die Scripts mit ersetzten Variablenwerten mit Hilfe der Profilerstellung generiert haben, befinden sich diese in dem Ausgabeverzeichnis, das Sie bei der Erstellung des Profils (standardmäßig `application_server-stammverzeichnis/profiles/<profile>/dbscripts/Cognos`) ausgewählt haben.
3. Führen Sie in der Befehlszeilenschnittstelle das Script durch den folgenden Befehl für Ihre Datenbanksoftware aus.
  - **DB2:** `db2 -tf createDatabase.sql`.
  - **DB2 for z/OS:** `db2 -tf createDatabase_Cognos.sql`. Das Datenbankskript kann mit einem der Dienstprogramme SPUFI oder DSNTEP2 ausgeführt werden.
  - **Oracle:** `sqlplus dbadmin/kennwort @ datenbankname @createDatabase.sql`. Dabei gilt:
    - `dbadmin` ist ein Oracle-Benutzer mit Administratorberechtigung.
    - `datenbankname` ist die Oracle-ID (z. B. `orcl`).
  - **Microsoft SQL Server:** `sqlcmd -U dbadmin -P kennwort -e -i createDatabase.sql`. Dabei gilt:
    - `dbadmin` ist ein SQL Server-Benutzer mit Administratorberechtigung
4. **Nur für DB2 for z/OS:**
  - a. In DB2 unter z/OS müssen Sie Tabellenbereiche mithilfe der IBM Cognos BI-Scripts `tablespace_db2z0S.sql` und `NC_TABLESPACES.sql` erstellen. Die vollständige Anleitung hierzu finden Sie im Information Center für IBM Cognos BI:

Vorgeschlagene Einstellungen für die Erstellung des Content-Store in DB2 unter z/OS

Tabellenbereiche für einen DB2-Content-Store unter z/OS erstellen

- b. Wenn IBM Cognos BI zum ersten Mal startet, erstellt es die Tabellen mithilfe folgender Scripts:

```
COGNOS_speicherposition/configuration/schemas/content/db2z0S/  
dbInitTest_db2z0S.sql
```

```
COGNOS_speicherposition/configuration/schemas/content/db2z0S/  
dbInitScript_db2z0S.sql
```

```
COGNOS_speicherposition/configuration/schemas/content/db2z0S/  
dbInitLock_db2z0S.sql
```

```
COGNOS_speicherposition/configuration/schemas/content/db2z0S/  
dbInitMeta_db2z0S.sql
```

```
COGNOS_speicherposition/configuration/schemas/delivery/zosdb2/  
NC_CREATE_DB2.sql
```

In Network Deployment-Umgebungen (ND) werden diese Dateien beim ersten Serverstart aus dem Master-Installationsverzeichnis für IBM Cognos BI in das entsprechende Serververzeichnis kopiert. Stellen Sie sicher, dass Sie die umgebungsspezifischen Variablen in diesen Dateien entsprechend ersetzt haben, bevor der IBM Cognos BI-Server startet; sonst verursachen die Tabellenerstellungsscripts Fehler, wenn der Server startet. Zur Bestimmung Ihrer *COGNOS\_speicherposition* siehe Ihr IBM Cognos BI-Stammverzeichnis zur Laufzeit suchen.

5. Starten Sie WebSphere Application Server.

---

## Tabellen für Messaging-Steuerkomponente manuell erstellen

Wenn die SI-Bus-Tabellen (SI = Service Integration) für die Messaging-Steuerkomponente von IBM Business Monitor während der Erstellung eigenständiger Profile oder bei Verwendung des Konfigurationsassistenten der Implementierungsumgebung oder des Konfigurationsassistenten nicht automatisch erstellt wurden, müssen Sie die Tabellen manuell erstellen. Sie müssen die Tabellen ferner dann manuell erstellen, wenn Sie DB2 for z/OS für den Datenspeicher der Messaging-Steuerkomponente verwenden.

Sie können auch eine CEI-Tabelle (CEI = Common Event Infrastructure) für die Messaging-Steuerkomponente erstellen. Bei der Erstellung der -Implementierungsumgebung werden die Datenbankskripts für die CEI generiert. Wenn Sie den CEI-Ereignisspeicher aktivieren möchten (in Produktionsumgebungen nicht empfohlen), müssen Sie die Scripts manuell ausführen, um die Konfiguration abzuschließen.

Verwenden Sie das Datenbankentwurfstool (DbDesignGenerator), um Scripts für die SI-Bus-Tabellen in Version 8.0 zu erstellen.

Alternativ können Sie auch 'sibDDLGenerator' verwenden. Der Befehl zum Generieren von SIB-DDL-Scripts für DB2 for z/OS lautet `sibDDLGenerator -system db2 -version 8.1 -platform zos`.

In der Dokumentation zu 'sibDDLGenerator' werden die unterstützten Versionen von DB2 aufgeführt. Es werden nicht alle von IBM Business Monitor unterstützten DB2-Versionen aufgelistet. Sie können Version 8.1 jedoch wie im Beispiel oben ersichtlich angeben. Die resultierende DDL dürfte mit allen unterstützten Versionen kompatibel sein.

Da IBM Business Monitor über eine CEI-Messaging-Steuerkomponente und auch über eine IBM Business Monitor-Messaging-Steuerkomponente verfügen kann, die beide mit demselben Tabellenbereich und denselben Tabellennamen erstellt werden, müssen Sie sicherstellen, dass entweder zwei unterschiedliche Datenbanken oder zwei unterschiedliche Schemanamen verwendet werden.

---

## Scripts für die Erstellung von Datenbankobjekten in DB2 for z/OS generieren

Wenn Sie eine Datenbankentwurfsdatei haben, können Sie diese zum Generieren von Datenbankskripts zur Erstellung von IBM Business Monitor-Datenbankobjekten in einem DB2 for z/OS-Datenbanksystem verwenden.

Installieren Sie IBM Business Monitor.

Stellen Sie sicher, dass Sie die entsprechenden Dateiberechtigungen zum Erstellen der Datenbankentwurfsdatei und der Datenbankskripts an den vorgesehenen Positionen besitzen.

Um die Datenbankskripts für die Erstellung Ihrer Datenbankobjekte zu generieren, können Sie das Datenbankentwurfstool mit dem Befehlszeilenparameter **-g** im unbeaufsichtigten Modus ausführen. In diesem Modus benötigt das Tool eine Eingabe aus einer Datenbankentwurfsdatei, in der die Konfiguration für Ihre DB2 for z/OS-Datenbank definiert ist. Die Datenbankentwurfsdatei muss bereits vorhanden sein, damit die Datenbankskripts generiert werden können.

Sie können das Datenbankentwurfstool im interaktiven Modus ausführen, um eine Datenbankentwurfsdatei zu generieren. Befolgen Sie die Bedienungshinweise des Tools, um eine DB2 for z/OS-Datenbankkonfiguration für Ihre eigenständige oder Network Deployment-Topologie zu definieren.

Bei der Definition einer DB2 for z/OS-Datenbankkonfiguration können Sie angeben, wie die SQL-Datenbankskripts gruppiert werden sollen, die Sie für die IBM Business Monitor-Komponenten generieren wollen. Bei Verwendung der Standardeinstellung werden die Skripts für jede Komponente in einem separaten Verzeichnis generiert. Legen Sie vor Ausführung des Datenbankentwurfstools eine Position fest, an der die vom Tool generierten Dateien gespeichert werden sollen.

Es müssen unbedingt ein Verzeichnispfad und eine Verzeichnisstruktur verwendet werden, die das Verfahren für die Verteilung der Datenbankobjekte im DB2 for z/OS-Subsystem reflektieren. Verwenden Sie für jede zu erstellende Datenbank ein einziges Ausgabeverzeichnis und generieren Sie in diesem Verzeichnis das gesamte Schema, das für die Erstellung der Datenbank erforderlich ist. Als Bezugshilfe können Sie den Namen des SQL-Verzeichnisses auch in Anlehnung an den Namen der Datenbank wählen, die Sie erstellen wollen.

Wenn Sie beispielsweise eine einzelne Datenbank namens W1MYDB erstellen wollen, können Sie die Datenbankskripts für alle Datenbankkomponenten gemeinsam im Verzeichnis `WAS_HOME/profiles/default/dbscripts/DB2-zOS/W1MYDB` generieren. Falls Sie zwei Datenbanken im Geltungsbereich der Zellenebene und der Clusterebene benötigen, können Sie das Datenbankschema wie im folgenden Beispiel gezeigt strukturieren:

- Um eine Datenbank namens W8CELLDB zu erstellen, die Datenbankobjekte mit einem Gültigkeitsbereich auf Zellenebene enthält, generieren Sie die Datenbankskripts für die MONITOR-Datenbankkomponente in einem Verzeichnis wie

WAS\_HOME/profiles/default/dbscripts/DB2-zOS/W8CELLDB. Später können Sie das generierte Schema zum Erstellen der Datenbankobjekte für die MONITOR-Datenbankkomponente in der Datenbank W8CELLDB ausführen. \*

- Um eine Datenbank namens W8S1DB zu erstellen, die die Datenbankobjekte mit einem Gültigkeitsbereich auf Clusterebene enthält, generieren Sie die Datenbankskripts für alle übrigen IBM Business Monitor-Komponenten in einem Verzeichnis wie WAS\_HOME/profiles/default/dbscripts/DB2-zOS/W8S1DB. Später können Sie das generierte Schema zum Erstellen der Datenbankobjekte für diese Komponenten in der Datenbank W8S1DB ausführen.

1. Kopieren Sie (sofern erforderlich) die Datenbankentwurfsdatei, die Ihre DB2 for z/OS-Konfiguration definiert, auf die Workstation, auf der IBM Business Monitor installiert ist, damit die Datei vom Befehl **DbDesignGenerator** verwendet werden kann.

2. Wechseln Sie in das IBM Business Monitor-Verzeichnis, in dem der Befehl **DbDesignGenerator** gespeichert ist:

```
cd WAS_HOME/util/dbUtils
```

Beispiel: `cd /WebSphere/V8T8DM/DeploymentManager/util/dbUtils`

3. Führen Sie den Befehl **DbDesignGenerator** mit der folgenden Syntax aus:

```
./DbDesignGenerator.sh -g datenbankentwurfsdatei
```

Hierbei steht *datenbankentwurfsdatei* für den vollständig qualifizierten Namen der Datenbankentwurfsdatei. Beispiel:

```
./DbDesignGenerator.sh -g /WebSphere/V8T8DM/DeploymentManager/profiles/default/dbscripts/DB2-zOS/W8CELL.nd.dbDesign
```

4. Prüfen Sie die in der Anzeige ausgegebenen Informationen, um sicherzustellen, dass keine Fehlernachrichten gemeldet werden. Für jede Datenbankkomponente gibt das Datenbankentwurfstool in der Anzeige Informationsnachrichten aus, die angeben, dass die Skripts in dem von der Datenbankentwurfsdatei angegebenen Verzeichnis generiert wurden. Für die MONITOR-Datenbankkomponente werden beispielsweise ähnliche Informationen wie im folgenden Beispiel angezeigt:

```
[Information] Die Skripts wurden erstellt in /WebSphere/V8T8DM/DeploymentManager/profiles/default
```

Nachdem die letzte Gruppe der Skripts generiert wurde, werden ähnliche Informationen wie im folgenden Beispiel ausgegeben:

```
[Information] Operation wird beendet...
```

**Tipp:** In der Datenbankentwurfsdatei sind die Verzeichnisse für die SQL-Skripts in jedem Komponentenabschnitt durch die Variable *ddl\_outDir* definiert. Falls Sie für die Generierung der SQL-Skripts eine andere Gruppe von Verzeichnissen verwenden wollen, besteht ein äußerst zeiteffizientes Verfahren darin, die Werte der Variablen *ddl\_outDir* manuell zu ändern. Anschließend speichern Sie die Datenbankentwurfsdatei und führen den Befehl **DbDesignGenerator** erneut so wie in Schritt 3 beschrieben aus.

Die folgenden Dateien werden erstellt:

- Die Datenbankskripts werden in einem oder mehreren angegebenen Verzeichnissen erstellt. Jedes Verzeichnis enthält außerdem ein Skript namens 'createDB2.sh', das Sie später zusammen mit den Datenbankskripts ausführen können, um die DB2 for z/OS-Datenbankobjekte zu erstellen.
- Es wird eine Protokolldatei mit dem Namen `dbDesignGenerator.log` in dem Verzeichnis erstellt, in dem Sie den Befehl **DbDesignGenerator.sh** aufgerufen haben.



---

## Datenbanken im DB2 for z/OS-Subsystem erstellen

Wenn Sie das Datenbankentwurfstool (**DbDesignGenerator**) zur Definition Ihrer Datenbankkonfiguration verwenden, können Sie die Datenbankskripts generieren, die zur Erstellung der Datenbanken für die IBM Business Monitor-Komponenten erforderlich sind.

Diese Datenbankskripts können mit verschiedenen Tools ausgeführt werden:

- Wenn Sie das Datenbankentwurfstool ausführen, um die Datenbankskripts zu generieren, wird auch das Script **createDB2.sh** generiert. Mit dem Script **createDB2.sh** können Sie die Datenbankskripts ausführen.
- Sie können Tools wie den DB2-Befehlszeilenprozessor (CLP), SPUFI oder DSNTEP2 zur Ausführung der Datenbankskripts verwenden.

### Zu verwendendes Tool auswählen

Sie können je nach Erfahrung und Vertrautheit oder auch nach persönlicher Präferenz ein Tool einem anderen Tool vorziehen. Es ist auch möglich, dass Ihr Unternehmen Standards oder Konventionen für die Tools festgelegt hat, die zum Erstellen von DB2 for z/OS-Objekten, insbesondere in einer Produktionsumgebung, zu verwenden sind.

### Hinweise zur Auswahl des Scripts 'createDB2.sh'

- **createDB2.sh** kann alle Datenbankobjekte durch eine einfache Ausführung des Tools erstellen, sodass dieses Script für eine erste Serverimplementierung eine gute Wahl ist.
- **createDB2.sh** führt die vom Datenbankentwurfstool (**DbDesignGenerator**) generierten Datenbankskripts aus.
- **createDB2.sh** führt das SQL für jede Komponente in der korrekten Reihenfolge aus.
- **createDB2.sh** erstellt Datenbankobjekte gemäß den von Ihnen definierten Namenskonventionen.
- **createDB2.sh** organisiert das Layout von Datenbankobjekten über DB2 for z/OS-Datenbanken hinweg.
- **createDB2.sh** erteilt Berechtigungen für Datenbank-, Speichergruppen- und Pufferpoolobjekte mit GRANT.
- **createDB2.sh** führt automatisch eine Anpassung der DDL-Anweisungen (Data Definition Language) für den Service Integration Bus aus.
- **createDB2.sh** wird in einer UNIX System Services-Umgebung ausgeführt.
- **createDB2.sh** generiert eine Prüfliste der Objekte, die erstellt werden.

### Hinweise zur Auswahl anderer Tools

- Sie bevorzugen vielleicht den DB2-Befehlszeilenprozessor (CLP) zur Ausführung der SQL-Anweisungen in der UNIX Systems Services-Umgebung. Sie müssen zuerst das Script **createDB2.sh** in einem Modus ausführen, der die Ausführung der SQL-Anweisungen übergeht und diese stattdessen in zwei .sql-Dateien zusammenstellt. Anschließend können Sie diese Dateien über den Befehlszeilenprozessor ausführen.
- Abgesehen von den Standardeinschränkungen für Datenbanksysteme besteht keine Einschränkung in Bezug auf die Benennungs- oder Organisationskonventionen, die für die Datenbankobjekte gelten.
- Einige Tools können in einer z/OS-Umgebung ausgeführt werden.

- Die Tools können eine Prüfliste der DB2-Datenbankbefehle generieren, die ausgeführt wurden.

## Aliasnamensdefinitionen für die Verbindung zum DB2 for z/OS-Server einrichten

Bevor Sie das Script **createDB2.sh** ausführen, müssen Sie den DB2-Befehlszeilenprozessor konfigurieren. Hierzu definieren Sie eine Gruppe von Umgebungsvariablen und einen Befehlsaliasnamen **db2**. Darüber hinaus müssen Sie Aliasnamen definieren, die zum Herstellen der Verbindung zum DB2 for z/OS-Server verwendet werden können.

Stellen Sie sicher, dass eine Eigenschaftendatei (z. B. `clp.properties`) für den DB2-Befehlszeilenprozessor vorhanden ist. Bei Bedarf können Sie ausgehend von der Beispielseigenschaftendatei, die in dem Verzeichnis verfügbar ist, in dem der Befehlszeilenprozessor installiert ist, eine eigene Eigenschaftendatei erstellen. Weitere Informationen enthält die Dokumentation von DB2 for z/OS.

Führen Sie die folgenden Schritte in der z/OS-Umgebung für UNIX System Services aus, in der das Script **createDB2.sh** ausgeführt werden soll:

1. Konfigurieren Sie den DB2-Befehlszeilenprozessor für jede Benutzer-ID, die DB2 for z/OS über die Befehlszeile verwenden wird. Sie können die persönlichen oder gemeinsam genutzten Benutzerprofile folgendermaßen aktualisieren:
  - Ändern Sie die Umgebungsvariable `CLASSPATH` so, dass sie die Datei `clp.jar` enthält.
  - Definieren Sie mit der Umgebungsvariablen `CLPPROPERTIESFILE` den vollständig qualifizierten Namen der Eigenschaftendatei für den Befehlszeilenprozessor.
  - Definieren Sie den Befehl **db2** als Aliasnamen für den Befehl, mit dem der Befehlszeilenprozessor gestartet wird.
  - Geben Sie die Datei `DB2JccConfiguration.properties` an, in der die JDBC-Eigenschaften definiert sind, die auf den Befehlszeilenprozessor angewendet werden sollen.

Beim Hinzufügen der erforderlichen Einträge zur Datei `.profile` oder `/etc/profile` können Sie die folgende Syntax verwenden:

```
export CLPHOME=installationsverzeichnis_des_befehlszeilenprozessors
export CLASSPATH=$CLASSPATH:$CLPHOME/lib/clp.jar
export CLPPROPERTIESFILE=pfad_der_eigenschaftendatei_für_den_befehlszeilenprozessor
alias db2="java -Ddb2.jcc.propertiesFile=dateipfad/DB2JccConfiguration.properties com.ibm.db2.c
```

Zum Beispiel:

```
export CLPHOME=/shared/db2910_base
export CLASSPATH=$CLASSPATH:$CLPHOME/lib/clp.jar
export CLPPROPERTIESFILE=/wasv8config/clp.properties
alias db2="java -Ddb2.jcc.propertiesFile=/wasv8config/DB2JccConfiguration.properties com.ibm.db2.c
```

2. Definieren Sie in der Eigenschaftendatei für den Befehlszeilenprozessor Aliasnamen, mit denen die Verbindung zum DB2 for z/OS-Server hergestellt werden kann. Eine Aliasnamensdefinition umfasst die folgenden Einträge:
  - Eine URL, die den Domänennamen oder die IP-Adresse des Datenbankservers, den Port für die Empfangsbereitschaft des Servers, den bei der Installation definierten DB2-Positionsnamen sowie die Eigenschaft für die JDBC-Verbindung angibt. Die URL kann das Format `server:port/datenbank eigenschaft=wert` verwenden. Die Werte für den Port und die Eigenschaft sind optional. Der DB2-Positionsname muss in Großbuchstaben angegeben werden.



- Eine Benutzer-ID und ein zugehöriges Kennwort, mit denen die Verbindung zum DB2-Server hergestellt werden kann. Diese Benutzer-ID sollte der Benutzer-ID (mit Berechtigung SYSADM) entsprechen, mit der das Script **createDB2.sh** vom DB2-Systemadministrator ausgeführt wird.

Sie können die erforderlichen Einträge für Aliasnamen mit der folgenden Syntax zur Eigenschaftendatei hinzufügen:

```
DB2-ALIASNAME=URL,benutzer-id,kennwort
```

Beispiel:

```
DSNXWBD=localhost:9446/DSNXWBD,SYSADM1,SYSPWRD1
```

**Tipp:** Wenn Sie in der Eigenschaftendatei einen Wert für *DB2-ALIASNAME* definieren, müssen Sie darauf achten, die richtigen Verbindungsdetails anzugeben, um sicherzustellen, dass keine Verbindung zu einer falschen Datenbank hergestellt und deren Inhalt versehentlich überschrieben wird.

3. Konfigurieren Sie den DB2-Subsystemparameter DBACRVW, damit Benutzer-IDs mit der Berechtigung DBADM für eine Datenbank die folgenden Tasks für andere Benutzer-IDs ausführen können: Sichten für Tabellen in der Datenbank erstellen, Aliasnamen für Tabellen erstellen und MQTs erstellen. Mithilfe der CLIST (Command List - Befehlsliste) für die Installation können Sie auf die ISPF-Anzeige DSNTIPP zugreifen und das Feld DBADM CREATE AUTH aktualisieren, indem Sie den Wert 'DB2 ZPARM DBACRVW=YES' für dieses Feld festlegen.

Verwenden Sie das Script **createDB2.sh**, um entweder die SQL-Anweisungen zum Erstellen der Datenbankobjekte für eine angegebene Datenbank auszuführen oder um die SQL-Anweisungen in zwei Dateien `.sql` zu konsolidieren, die Sie später unter Verwendung anderer Datenbanktools ausführen können.

## DB2 for z/OS-Datenbankobjekte mit dem Script 'createDB2.sh' erstellen

Nach der Erstellung der Datenbankskripts für die IBM Business Monitor-Komponenten können Sie das Script **createDB2.sh** ausführen, um eine oder mehrere Datenbanken im DB2 for z/OS-Subsystem zu erstellen und die Datenbanken mit Objekten zu füllen.

Sie können auch Tools wie den DB2-Befehlszeilenprozessor (CLP), SPUFI oder DSNTPEP2 zum Erstellen und Füllen von Datenbanken verwenden.

- Legen Sie den Entwurf und die Konfiguration der DB2 for z/OS-Datenbank fest. Dies schließt auch die Anzahl der Datenbanken ein, die für die IBM Business Monitor-Komponenten benötigt werden. In einer eigenständigen Serverumgebung könnten Sie beispielsweise alle Komponentendatenbanken in einer einzigen DB2 for z/OS-Datenbank einrichten.
- Legen Sie eine Namenskonvention für die DB2 for z/OS-Objekte wie Datenbanken, Speichergruppen, VSAM-Katalognamen (VCATs), Schemapräfixe, Pufferpools und Sicherheits-IDs fest.
- Erstellen Sie die erforderlichen Pufferpools. Weitere Informationen finden Sie in Beispielen für DB2-Befehle und SQL.
- Führen Sie das Datenbankentwurfstool (**DbDesignGenerator**) aus, um die Datenbankskripts zu generieren, mit deren Hilfe die Datenbankobjekte für die IBM Business Monitor-Komponenten erstellt werden können. Richten Sie Ihre Datenbankkonfiguration so ein, dass das Datenbankentwurfstool für jede zu erstellende Datenbank ein einziges Ausgabeverzeichnis erstellt und alle relevanten Da-

tenbankscripts (inklusive des Scripts **createDB2.sh**), die für die Erstellung der Datenbank erforderlich sind, in diesem Verzeichnis generiert.

- Übertragen Sie die Datenbankskripts, einschließlich des Scripts **createDB2.sh**, per FTP auf das z/OS-System, das die DB2 for z/OS-Installation enthält. Übertragen Sie das Script **createDB2.sh** als ASCII-Textdatei. Verwenden Sie zur Übertragung der Datenbankschemadateien den Binärmodus. Stellen Sie außerdem sicher, dass die Verzeichnisstruktur beim Übertragen der Dateien erhalten bleibt.
- Erteilen Sie Ausführungsberechtigungen für das Script **createDB2.sh**.
- Erstellen oder erweitern Sie das Profil.
- Richten Sie Aliasnamensdefinitionen für die Verbindung zum DB2-Server ein.

Wie viele Datenbanken Sie für Ihre IBM Business Monitor-Installation erstellen können, kann von Ihrer Konfiguration sowie davon abhängig sein, wie Sie die Datenbankobjekte im DB2 for z/OS-Subsystem verteilen wollen. Unter der Voraussetzung, dass die Datenbankskripts ordnungsgemäß in den Ausgabeverzeichnissen gruppiert sind, die Sie beim Ausführen des Entwurfstools angegeben haben, können Sie das Script **createDB2.sh** ein Mal für jede zu erstellende Instanz einer Datenbank ausführen. Beispiel:

- Um eine einzige Datenbank zu erstellen, können Sie das Script **createDB2.sh** ein Mal in einem Verzeichnis ausführen, in dem alle Datenbankskripts enthalten sind, die für alle IBM Business Monitor-Komponenten generiert wurden.
- Um mehrere Datenbanken auf Zellen- und Clusterebene zu erstellen, können Sie das Script **createDB2.sh** ein Mal in jedem Verzeichnis ausführen, in dem die Datenbankskripts enthalten sind, die zum Erstellen der Datenbankobjekte für die Zelle und die Cluster benötigt werden.

**Wichtig:** Es wird davon ausgegangen, dass der DB2 for z/OS-Systemadministrator das Script **createDB2.sh** mit einer Benutzer-ID ausführt, die die Berechtigung SYS-ADM besitzt, um die Datenbanken und Speichergruppen zu erstellen. Anschließend kann der Systemadministrator die Berechtigung DBADM für die IBM Business Monitor-Datenbanken dem WebSphere-Administrator erteilen.

Führen Sie für jede Datenbank, die Sie erstellen wollen, die folgenden Schritte aus:

1. Greifen Sie auf dem z/OS-System, das die DB2-Installation enthält, auf die Befehlshell 'UNIX System Services' zu und wechseln Sie dann in das Verzeichnis, in das Sie die Datenbankskripts für die zu erstellenden Datenbankobjekte übertragen haben. Zum Beispiel:

```
cd /u/work/S4CELLDB
```

2. Führen Sie das Script **createDB2.sh** unter Verwendung der folgenden Syntax aus:

```
createDB2.sh -DBAlias aliasname -DBName datenbankname -DBSto  
speichergruppennamen -DBCcreate -DBVCat datenträgerkatalog -DBUser  
datenbankbenutzer-id -RunSQL
```

Hierbei gilt Folgendes:

**-DBAlias**

Gibt einen Aliasnamen an, der der DB2-Server-URL, der Benutzer-ID und dem Kennwort zugeordnet ist und der zum Herstellen der Verbindung zu DB2 verwendet wird. Falls Sie diesen Parameter bei der Ausführung des Scripts **createDB2.sh** nicht angeben, werden Sie zur Eingabe eines Wertes aufgefordert.

**-DBName**

Gibt den Namen der zu erstellenden Datenbank an.

**-DBSto**

Gibt den Namen der Speichergruppe für die Datenträger an, auf denen sich die Dateien befinden, in denen Tabellen und Indizes gespeichert sind.

**-DBCreate**

Erstellt die Datenbank.

**-DBVCat**

Gibt den Namen des Katalogs von DB2 Virtual Storage Access Method (VSAM) an, in dem Datensatzinformationen zu den Dateien aufgezeichnet werden.

**-DBUser**

Gibt die Benutzer-ID des WebSphere-Administrators an, der für die zu erstellende IBM Business Monitor-Datenbank eine Datenbankadministratorberechtigung besitzt.

**-RunSQL**

Führen Sie die SQL-Anweisungen aus, die die Datenbankobjekte erstellen.

Zum Beispiel:

```
createDB2.sh -DBAlias DSNXWBD -DBName S4CELLDB -DBSto S4DBSTO -DBCreate  
-DBVCat DSNV10PP -DBUser S4ADMIN -RunSQL Informationen zu allen Parametern,  
die für das Script createDB2.sh verfügbar sind, sowie ein Beispiel für seine  
Verwendung finden Sie in Script 'createDB2.sh'.
```

3. Prüfen Sie die in der Konsole angezeigten Nachrichten, um sicherzustellen, dass keine Fehlermeldungen ausgegeben wurden.

**Tipp:** Wenn Sie **createDB2.sh** erstmalig zum Erstellen einer Datenbank ausführen, werden einige wenige Nachrichten ausgegeben, weil das Script zunächst versucht, die Datenbank zu löschen, die zu diesem Zeitpunkt jedoch noch nicht vorhanden ist. Diese Nachrichten können Sie ignorieren. Bei nachfolgenden Aufrufen von **createDB2.sh** für dieselbe Datenbank werden diese Nachrichten nicht erneut ausgegeben.

Nachdem die Ausführung des Scripts abgeschlossen ist, können Sie auch die Datei `z_output.txt` überprüfen. Diese Datei enthält ein Prüfprotokoll der abgeschlossenen Operationen und Statusnachrichten. Sie ist in dem Verzeichnis gespeichert, in dem Sie das Script **createDB2.sh** ausgeführt haben.

Jede Datenbank wird erstellt und mit den erforderlichen Datenbankobjekten gefüllt.

## DB2 for z/OS-Datenbankobjekte über den DB2-Befehlszeilenprozessor erstellen

Wenn Sie das Script **createDB2.sh** ausführen, haben Sie die Wahl, ob das SQL unverzüglich ausgeführt werden soll, um die Datenbankobjekte für die angegebene Datenbank zu erstellen, oder ob die Ausführung der SQL-Skripts übergangen werden soll, sodass sie später ausgeführt werden können. Wenn Sie die Ausführung des SQL übergehen, stellt das Script **createDB2.sh** die SQL-Anweisungen in zwei Dateien (`z_schema.sql` und `z_schemaProc.sql`) zusammen, die Sie später über den DB2-Befehlszeilenprozessor (CLP) ausführen können.

Sie können diese `.sql`-Dateien auch mit einem anderen Datenbanktool Ihrer Wahl (z. B. SPUFI oder DSNTEP2) ausführen.

- Legen Sie den Entwurf und die Konfiguration der DB2 for z/OS-Datenbank fest. Dies schließt auch die Anzahl der Datenbanken ein, die für die IBM Business Monitor-Komponenten benötigt werden. In einer eigenständigen Serverumge-

bung könnten Sie beispielsweise alle Komponentendatenbanken in einer einzigen DB2 for z/OS-Datenbank einrichten.

- Legen Sie eine Namenskonvention für die DB2 for z/OS-Objekte wie Datenbanken, Speichergruppen, VSAM-Katalognamen (VCATs), Schemapräfixe, Pufferpools und Sicherheits-IDs fest.
- Erstellen Sie die erforderlichen Pufferpools. Weitere Informationen finden Sie in Beispielen für DB2-Befehle und SQL.
- Führen Sie das Datenbankentwurfstool (**DbDesignGenerator**) aus, um die Datenbankskripts zu generieren, mit deren Hilfe die Datenbankobjekte für die IBM Business Monitor-Komponenten erstellt werden können. Richten Sie Ihre Datenbankkonfiguration so ein, dass das Datenbankentwurfstool für jede zu erstellende Datenbank ein einziges Ausgabeverzeichnis erstellt und alle relevanten Datenbankskripts (inklusive des Skripts **createDB2.sh**), die für die Erstellung der Datenbank erforderlich sind, in diesem Verzeichnis generiert.
- Übertragen Sie die Datenbankskripts, einschließlich des Skripts **createDB2.sh**, per FTP auf das z/OS-System, das die DB2 for z/OS-Installation enthält. Übertragen Sie das Skript **createDB2.sh** als ASCII-Textdatei. Verwenden Sie zur Übertragung der Datenbankschemadateien den Binärmodus. Stellen Sie außerdem sicher, dass die Verzeichnisstruktur beim Übertragen der Dateien erhalten bleibt.
- Erteilen Sie Ausführungsberechtigungen für das Skript **createDB2.sh**.
- Erstellen oder erweitern Sie das Profil.
- Richten Sie Aliasnamensdefinitionen für die Verbindung zum DB2-Server ein.

Unter der Voraussetzung, dass die Datenbankskripts ordnungsgemäß in den Ausgabeverzeichnissen gruppiert sind, die Sie beim Ausführen des Entwurfstools angegeben haben, können Sie das Skript **createDB2.sh** ein Mal für jede zu erstellende Instanz einer Datenbank ausführen.

**Wichtig:** Es wird davon ausgegangen, dass der DB2 for z/OS-Systemadministrator das Skript **createDB2.sh** mit einer Benutzer-ID ausführt, die die Berechtigung SYSADM besitzt, um die Datenbanken und Speichergruppen zu erstellen. Anschließend kann der Systemadministrator die Berechtigung DBADM für die IBM Business Monitor-Datenbanken dem WebSphere-Administrator erteilen.

Führen Sie für jede Datenbank, die Sie erstellen wollen, die folgenden Schritte aus:

1. Greifen Sie auf dem z/OS-System, das die DB2-Installation enthält, auf die Befehlshell 'UNIX System Services' zu und wechseln Sie dann in das Verzeichnis, in das Sie die Datenbankskripts für die zu erstellenden Datenbankobjekte übertragen haben. Zum Beispiel:

```
cd /u/work/S4CELLDB
```

2. Führen Sie das Skript **createDB2.sh** unter Verwendung der folgenden Syntax aus:

```
createDB2.sh -DBAlias aliasname -DBName datenbankname -DBSto  
speichergruppennamen -DBCreate -DBVCat datenträgerkatalog -DBUser  
datenbankbenutzer-id
```

Hierbei gilt Folgendes:

**-DBAlias**

Gibt einen Aliasnamen an, der der DB2-Server-URL, der Benutzer-ID und dem Kennwort zugeordnet ist und der zum Herstellen der Verbindung zu DB2 verwendet wird. Falls Sie diesen Parameter bei der Ausführung des Skripts **createDB2.sh** nicht angeben, werden Sie zur Eingabe eines Wertes aufgefordert.

**-DBName**

Gibt den Namen der zu erstellenden Datenbank an.

**-DBSto**

Gibt den Namen der Speichergruppe für die Datenträger an, auf denen sich die Dateien befinden, in denen Tabellen und Indizes gespeichert sind.

**-DBCreate**

Erstellt die Datenbank.

**-DBVCat**

Gibt den Namen des Katalogs von DB2 Virtual Storage Access Method (VSAM) an, in dem Datensatzinformationen zu den Dateien aufgezeichnet werden.

**-DBUser**

Gibt die Benutzer-ID des WebSphere-Administrators an, der für die zu erstellende IBM Business Monitor-Datenbank eine Datenbankadministratorberechtigung besitzt.

**Tipp:** Durch Weglassen des Parameters **-RunSQL** übergehen Sie die Ausführung der SQL-Anweisungen, die die Datenbankobjekte erstellen. Stattdessen werden die Anweisungen in zwei `.sql`-Dateien zusammengestellt.

Beispiel:

```
createDB2.sh -DBAlias DSNXWBD -DBName S4CELLDB -DBSto S4DBSTO -DBCreate
-DBVCat DSNV10PP -DBUser S4ADMIN Informationen zu allen Parametern, die für
das Script createDB2.sh verfügbar sind, sowie ein Beispiel für seine Verwen-
dung finden Sie in Script 'createDB2.sh'.
```

Die Dateien `z_schema.sql` und `z_schemaProc.sql`, in denen sich die zusammen-  
gestellten SQL-Anweisungen befinden, werden in dem Verzeichnis generiert, in  
dem Sie das Script **createDB2.sh** ausgeführt haben. Die Datei `z_schemaProc.sql`  
enthält SQL-Anweisungen für gespeicherte Prozeduren und wird zusätzlich zur  
Datei `z_schema.sql` generiert, weil für gespeicherte Prozeduren das kommerzi-  
elle A (@) als Anweisungsabschlusszeichen bei der Ausführung des Befehlszei-  
lenprozessors erforderlich ist.

3. Führen Sie den DB2-Befehlszeilenprozessor im Stapelmodus aus, um das SQL in der Datei `z_schema.sql` auszuführen:

```
db2 -f /pfad_von_createDB2.sh/z_schema.sql
```

Beispiel:

```
db2 -f /u/work/S4CELLDB/z_schema.sql Der Befehlszeilenprozessor liest die
Daten in der Datei und verarbeitet die Befehle in der Datei nacheinander.
```

4. Führen Sie den DB2-Befehlszeilenprozessor erneut aus, um das SQL in der Datei `z_schemaProc.sql` auszuführen. Verwenden Sie zusätzlich den Parameter **-td**, um das Zeichen '@' als Anweisungsabschlusszeichen zu definieren.

```
db2 -td@ -f /pfad_von_createDB2.sh/z_schemaProc.sql
```

Beispiel:

```
db2 -td@ -f /u/work/S4CELLDB/z_schemaProc.sql
```

Jede Datenbank wird erstellt und mit den erforderlichen Datenbankobjekten gefüllt.

---

## Hinweise zur Einrichtung und Konfiguration von High Availability Disaster Recovery (HADR)

Prüfen Sie die Hinweise in diesem Abschnitt, wenn Sie planen, DB2 für High Availability Disaster Recovery (HADR) einzurichten und zu konfigurieren.

- „Status von Datenbanken für Übernahme prüfen“
- „Datenquellen für HADR konfigurieren“
- „Programmgestützte Transaktionswiederholungseigenschaften“
- „Benutzeraufgabenbereiche für HADR angeben“ auf Seite 81
- „Messaging-Steuerkomponente nach Übernahme starten“ auf Seite 81
- „Auf weitere Informationen zugreifen“ auf Seite 82

### Status von Datenbanken für Übernahme prüfen

Wenn an einem Standort eine Störung auftritt, kann die Bereitschaftsdatenbank durch High Availability Disaster Recovery (HADR) die Aufgabe der Primärdatenbank mit voller DB2-Funktionalität übernehmen. Bevor die Übernahme stattfindet, überprüfen Sie den HADR-Status von DB2 sowohl für die Primärdatenbank als auch für die Bereitschaftsdatenbank, um festzustellen, ob die Übernahme zulässig ist oder ob ein Fehler zurückgegeben wird. Die Übernahme kann manchmal einen Fehler verursachen oder möglicherweise nicht zulässig sein.

Weitere Informationen finden Sie im Abschnitt zum HADR-Befehl TAKEOVER. Prüfen Sie die Befehlsparameter und die Hinweise zur Verwendung, ob festzustellen, ob die Übernahme ausführbar ist.

### Datenquellen für HADR konfigurieren

Konfigurieren Sie die DB2-Datenquellen für High Availability Disaster Recovery (HADR) in der Administrationskonsole von IBM Business Manager, wie im Abschnitt Clientweiterleitung für Anwendungen konfigurieren, die DB2-Datenbanken verwenden beschrieben.

Beachten Sie bei der Konfiguration der Datenquellen für IBM Business Process Manager-Produkte die folgenden Hinweise:

- Es wird empfohlen, die automatische Clientweiterleitung zu aktivieren, wenn HADR für DB2 eingerichtet wird.
- Für Datenquellen auf der Ebene der Messaging-Steuerkomponente und auf Zelebene müssen die Eigenschaften *Alternative Servernamen* und *Alternative Portnummern* konfiguriert werden.
- Der alternative Port muss der externe Port für den DB2-Server sein. Es darf sich nicht um den HADR-Service-Port handeln, der in `/etc/services` angegeben ist. Ist beispielsweise der HADR-Service-Port `DB2_HADR_1` in `/etc/services` mit der Nummer 55001 angegeben und verwendet der DB2-Server den externen Port 50000, müssen Sie in der Administrationskonsole den Port 50000 als alternativen Port für die Datenquelle angeben.

### Programmgestützte Transaktionswiederholungseigenschaften

Zur Unterstützung programmgestützter Transaktionswiederholungen wurden zwei neue Eigenschaften in der Datei `00static.xml` mit den folgenden Werten hinzugefügt:



```
<transaction-reroute-retries>3</transaction-reroute-retries>
<transaction-reroute-retry-delay-in-millis>10000</transaction-reroute-retry-delay-in-millis>
```

Passen Sie in der Konfigurationsdatei 100Custom.xml die Änderungen in 00Static.xml an, wenn andere Werte als die Standardwerte erforderlich sind. Führen Sie die folgenden Schritte aus:

1. Lokalisieren Sie die Konfigurationsdatei 100Custom.xml:

- Für eine Network Deployment-Umgebung ist der Dateipfad: <DMGR-profilstammverz>\config\cells\<zellenname>\nodes\<angepasster\_knotenname>\servers\<servername>\servertyp\config\100Custom.xml.
- Für eine eigenständige Serverumgebung ist der Dateipfad: <stammverz\_des\_eigenständigen\_profil>\config\cells\<zellenname>\nodes\<name\_des\_eigenständigen\_knotens>\servers\<servername>\server\_type\config\100Custom.xml.

2. Bearbeiten Sie die Datei 100Custom.xml. Bearbeiten Sie den folgenden Abschnitt, sodass er wie in diesem Beispiel gezeigt aussieht:

```
<server merge="mergeChildren">
  <transaction-reroute-retries merge="replace">10</transaction-reroute-retries>
  <transaction-reroute-retry-delay-in-millis merge="replace">3000</transaction-reroute-retry-d
</server>
```

3. Speichern Sie Ihre Änderungen.

Geben Sie alle Clientweiterleitungseigenschaften für alle Ihre Datenquellen an.

## Benutzeraufgabenbereiche für HADR angeben

Geben Sie bei der Einrichtung von High Availability Disaster Recovery (HADR) geeignete Benutzeraufgabenbereiche pro Plattform an, um festzulegen, welche HA-DR-Tasks die verschiedenen Benutzer ausführen können.

- Verwenden Sie bei Windows den DB2-Benutzer mit Verwaltungsaufgaben: db2admin
- Verwenden Sie bei Linux den DB2-Instanzbenutzer db2inst1 anstelle des Benutzers mit Verwaltungsaufgaben (dasusr1).

Wenn beispielsweise der DB2-Instanzbenutzer angegeben ist, sichert der Benutzer db2inst1 die Primärdatenbank, kopiert das Sicherungsbild auf den Bereitschaftsdatenbankserver und stellt anschließend den Bereitschaftsdatenbankserver unter Verwendung dieses Bildes wieder her bzw. startet ihn mit diesem Image. Ist der Benutzer mit Verwaltungsaufgaben angegeben, ist der Benutzer dasusr1 der Eigner des kopierten Bildes, auf das der Benutzer db2inst1, der die Sicherung und Wiederherstellung ausführt, keinen Zugriff hat. Da die beiden Benutzer zu verschiedenen Gruppen gehören und unterschiedliche Zugriffsberechtigungen für Dateien besitzen, schlägt die HADR-Einrichtung möglicherweise fehl.

## Messaging-Steuerkomponente nach Übernahme starten

Wenn der automatische Neustart der Messaging-Steuerkomponente inaktiviert ist, müssen Sie die Messaging-Steuerkomponente nach der Datenbankübernahme manuell starten.

Wenn zwei Server für Messaging-Steuerkomponenten in demselben Cluster vorhanden sind, wobei der Messaging-Server 1 einen aktiven Status und der Messa-

ging-Server 2 einen verknüpften Status aufweist, ist aufgrund der folgenden Ereignissequenz möglicherweise kein Server für Messaging-Steuerkomponenten in Ihrer Umgebung aktiv:

1. Die Datenbank, die von den Messaging-Steuerkomponenten verwendet wurde, wurde übernommen.
2. Der Messaging-Server 1 wurde heruntergefahren, um einen Datenverlust zu verhindern.
3. Messaging-Server 2 hat alle Messaging-Steuerkomponenten gestartet und fungiert als aktiver Server, während Messaging-Server 1 weiterhin inaktiv ist.
4. Es hat eine weitere Übernahme der Datenbank stattgefunden.
5. Der Messaging-Server 2 wurde heruntergefahren, um einen Datenverlust zu verhindern.
6. Beide Messaging-Server (1 und 2) sind inaktiv.

### **Auf weitere Informationen zugreifen**

Wenn Sie weitere Informationen benötigen, verwenden Sie die folgenden Links.

- Wenn ein Ausfall in Ihrer DB2-HADR-Umgebung auftritt: Systemausfälle in einer Hochverfügbarkeitslösung erkennen und darauf reagieren.
- Wenn die Funktionsübernahme stattgefunden hat und der DB2-HADR-Status nicht Peer ist und einiger Datenverlust auftritt, konfigurieren Sie den DB2-HADR-Status mit Peer, wie in den folgenden Abschnitten beschrieben:
  - Ausführen einer HADR-Funktionsübernahmeoperation
  - Erneutes Integrieren einer Datenbank nach einer Übernahmeoperation

---

## **Oracle Real Application Cluster (RAC) zur Verwendung mit IBM Business Monitor konfigurieren**

Oracle Real Application Clusters (RAC) ist eine Option einer Oracle-Datenbank, die zwei oder mehr Computer zusammenführt, um daraus eine Clusterdatenbank zu bilden, die sich wie ein einziges System verhält. In einer RAC-Datenbank greifen Oracle-Prozesse, die auf separaten Knoten ausgeführt werden, auf dieselben Daten auf einem gemeinsam genutzten Plattenspeicher zu.

Wenn Sie IBM Business Monitor-Profile mit Oracle erstellen, geben Sie den Host und den Port eines der RAC-Server sowie den Servicennamen des RAC-Service als Datenbanknamen ein.

Wenn die Systeme später aktiv sind, führen Sie die Konfigurationsschritte aus, um die WebSphere-Datenquellen zu ändern, die eine Verbindung zum Oracle RAC mit dem RAC-Servicennamen herstellen sollen.

Abhängig von der Version von Oracle RAC, die Sie mit IBM Business Monitor verwenden, müssen Sie möglicherweise einige Konfigurationsschritte ausführen.

- Falls Sie Oracle 11g R2 mit der Funktion SCAN verwenden, ist für IBM Business Monitor keine zusätzliche manuelle Konfiguration erforderlich, sofern Sie während der Profilerstellung oder der Topologiekonfiguration den Servicennamen angeben. Die während der Konfiguration generierte JDBC-URL hat das Format `jdbc:oracle:thin:@//[SCAN_LISTENER_HOST][:SCAN_LISTENER_PORT]/SERVICE` und funktioniert für Oracle RAC ohne manuelle Aktualisierungen ordnungsgemäß.
- Falls Sie die Funktion SCAN nicht verwenden wollen oder eine frühere Oracle-Version nutzen, die die Funktion SCAN nicht unterstützt, müssen Sie die Konfi-



gurationsschritte in der beschriebenen Vorgehensweise ausführen, um IBM Business Monitor für die Verwendung mit Oracle RAC zu konfigurieren.

Zwei Szenarios sind möglich:

- Bei Verwendung eines eigenständigen Profils müssen Sie das Profil unter Verwendung der SID als Wert für den Datenbanknamen erstellen.
- Bei Einrichtung einer Network Deployment-Umgebung müssen die Profile und Cluster unter Verwendung der SID konfiguriert werden.

IBM Business Monitor erstellt die JDBC-URL immer im folgenden Format:

```
jdbc:oracle:thin:@//[SCAN_LISTENER_HOST][:SCAN_LISTENER_PORT]/SERVICE
```

Sie können dieses Format für die Verwendung mit Oracle RAC bearbeiten:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=rac-knoten1)(PORT=1521))
(ADDRESS=(PROTOCOL=TCP)(HOST=rac-knoten2)(PORT=1521))
(FAILOVER=on)(LOAD_BALANCE=on)
(CONNECT_DATA=(SERVER=DEDICATED)
(SERVICE_NAME=servicename)))
```

Geben Sie beim Definieren der relevanten Oracle-JDBC-Datenquellen die RAC-URL als Oracle-URL an:

1. Wählen Sie in der Administrationskonsole die Optionen **Ressourcen > JDBC > Datenquellen** aus.
2. Bearbeiten Sie alle Datenquellen, die Oracle mit der JDBC-URL verwenden, so, dass eines der im Abschnitt „Informationen zu diesem Vorgang“ gezeigten Formate verwendet wird.

Wenn Sie IBM Cognos BI verwenden, nachdem die Systeme erneut gestartet wurden und funktionieren, können die IBM Business Monitor-Cubes (Würfel) veröffentlicht werden. Wenn der erste Cube veröffentlicht ist, wird die Datenquelle WBMONITOR\_DB in IBM Cognos BI mit der Oracle RAC-URL erstellt, die jetzt von der WebSphere-Datenquelle verwendet wird.

Wenn die Cubes vor der Änderung in der Oracle RAC-URL veröffentlicht wurden, führen Sie die folgenden Schritte aus:

1. Entfernen Sie in IBM Cognos BI die Datenquelle WBMONITOR\_DB über **IBM Cognos Administration**.
2. Veröffentlichen Sie die Cubes erneut, um die IBM Cognos BI-Verbindung mit der Oracle RAC-URL neu zu erstellen.

---

## Oracle Data Guard für IBM Business Monitor konfigurieren

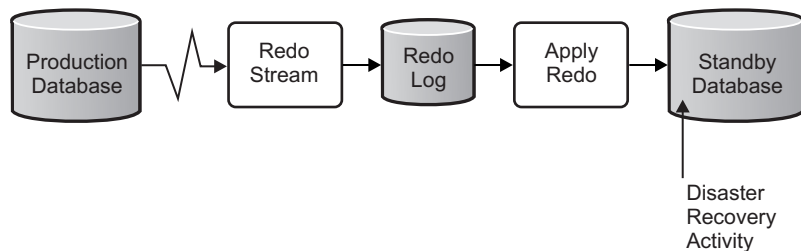
Sie können Oracle Data Guard für die Verwendung mit IBM Business Monitor konfigurieren. Oracle Data Guard stellt Funktionalität für hohe Verfügbarkeit, Notfallwiederherstellung und Datenschutz bereit und dient zur Erstellung, Verwaltung und Überwachung einer oder mehrerer Bereitschaftsdatenbanken (Standby-Datenbanken), sodass Oracle-Datenbanken in Produktionsumgebungen gegen Katastrophen und Datenverluste abgesichert werden.

Wenn IBM Business Monitor zur Verwendung von Oracle Data Guard konfiguriert ist, haben Sie in der Regel eine Produktionsdatenbank, die Ihre Primärdatenbank ist, und mehrere Bereitschaftsdatenbanken. In diesem Fall verwaltet Oracle Data Guard jede Bereitschaftsdatenbank automatisch, indem Wiederholungsdaten aus der Primärdatenbank übertragen und auf die Bereitschaftsdatenbank angewendet werden. Wenn Ihre Produktionsdatenbank aufgrund einer geplanten oder unge-

planten Betriebsunterbrechung nicht verfügbar ist, bietet Ihnen Oracle Data Guard die Möglichkeit, eine beliebige Bereitschaftsdatenbank in die Rolle der Produktionsdatenbank zu versetzen, sodass die mit der Betriebsunterbrechung verbundene Ausfallzeit minimiert wird.

Oracle Data Guard verwaltet jede Bereitschaftsdatenbank automatisch durch die Übertragung von Wiederholungsdaten aus der Primärdatenbank und die Anwendung dieser Wiederholungsdaten auf die Bereitschaftsdatenbank.

### Eine typische Data Guard-Konfiguration



1. Richten Sie die Oracle Data Guard-Umgebung ein.
2. Erstellen Sie einen Datenbankservice mit der Primärdatenbank:  
`Exec DBMS_SERVICE.CREATE_SERVICE('BPM', 'BPM');`
3. Erstellen Sie einen Trigger in der Primärdatenbank, indem Sie den folgenden Befehl ausführen:

```
CREATE OR REPLACE TRIGGER START_SERVICES AFTER STARTUP ON DATABASE DECLARE ROLE VARCHAR(30);BEGIN
```

**Anmerkung:** Wenn Sie eine Datenbank starten, startet Ihre Primärdatenbank immer einen BPM-Service. Daher stellt Ihr Client immer eine Verbindung zu Primärdatenbank her.

4. Starten Sie die Primärdatenbank erneut oder starten Sie den folgenden Service durch den folgenden Befehl:  
`EXEC DBMS_SERVICE.START_SERVICE('BPM');`
5. Installieren Sie IBM Business Monitor.
6. Erstellen Sie Profile oder eine Implementierungsumgebung, die einer Oracle-Instanzdatenbank ähnlich ist. Wählen Sie bei der Erstellung des Profils die Option **Oracle-Datenbank** aus und stellen Sie eine Verbindung zu dem Datenbankservice her, den Sie in Schritt 2 erstellt haben.

Wenn Ihre Primärdatenbank und alle Bereitschaftsdatenbanken auf demselben Server installiert sind, verwenden die Datenbanken die gleiche IP-Adresse und den gleichen Oracle-Empfangsport. Es ist keine weitere Konfiguration erforderlich.

Wenn Ihre Primärdatenbank und Ihre Bereitschaftsdatenbanken hingegen auf verschiedenen Servern installiert sind, haben sie unterschiedliche IP-Adressen und denselben Oracle-Empfangsport. Wenn sich Ihre Primärdatenbank und Ihre Bereitschaftsdatenbanken auf separaten Servern befinden, müssen Sie alle Datenquellen ändern, sodass Sie eine JDBC-URL ähnlich der nachfolgend beschriebenen URL haben.

Gehen Sie wie folgt vor, um die JDBC-URL zu ändern:

1. Melden Sie sich bei der Administrationskonsole von IBM Business Monitor an.
2. Wählen Sie **Ressourcen > JDBC > Datenquellen** aus.

3. Ändern Sie alle Datenquellen, die eine Verbindung zu der Oracle-Datenbank herstellen, und geben Sie für diese Datenquellen URLs ähnlich der folgenden URL an:

```
jdbc:oracle:thin:@(DESCRIPTION=
  (ADDRESS_LIST=
    (ADDRESS=(PROTOCOL=TCP)(HOST=<host A>)(PORT=1521))
    (ADDRESS=(PROTOCOL=TCP)(HOST=<host B>)(PORT=1521))
    (ADDRESS=(PROTOCOL=TCP)(HOST=<host C>)(PORT=1521))
    (LOAD_BALANCE=off)
    (FAILOVER=on)
  )
  (CONNECT_DATA=(SERVICE_NAME=BPM))
)
```



---

## Kapitel 6. Profile erstellen und erweitern

Nach der Installation von IBM Business Monitor muss mindestens ein Profil erstellt werden, um Ihre Laufzeitumgebung vorzubereiten. Sie können Profile entweder mithilfe des Profile Management Tools oder mit dem Befehl **manageprofiles** erstellen und erweitern.

Wenn Sie Solaris im 64-Bit-Modus verwenden, ist die Benutzerschnittstelle des Profile Management Tools nicht verfügbar. Sie müssen den Befehl **manageprofiles** verwenden. Bei Verwendung von z/OS können Sie weder den Befehl noch das Profile Management Tool verwenden. Lesen Sie in diesem Fall die Informationen im Abschnitt zum Erstellen allgemeiner Konfigurationen für IBM Business Monitor for z/OS.

Es gibt drei Profilarten: ein eigenständiges Serverprofil, ein Deployment Manager-Profil (ein Verwaltungsprofil mit einem Deployment Manager-Server) und ein angepasstes Profil (einen verwalteten Knoten). Jedes Profil definiert eine andere Laufzeitumgebung mit eigenen Dateien (Befehlen, Konfigurationsdateien und Protokolldateien).

---

### Profile mit dem Profile Management Tool erstellen und erweitern

Mit dem Profile Management Tool in WebSphere Customization Toolbox können Sie Profile für die Verwaltung Ihrer Laufzeitumgebung erstellen oder erweitern.

**Einschränkung:** Wenn Sie Solaris im 64-Bit-Modus verwenden, ist die Benutzerschnittstelle des Profile Management Tools nicht verfügbar. Sie müssen den Befehl **manageprofiles** verwenden. Wenn Sie mit z/OS arbeiten, dann lesen Sie die Informationen im Abschnitt zum Erstellen allgemeiner Konfigurationen für IBM Business Monitor for z/OS.

#### Windows

**Wichtig:** Um das Profile Management Tool unter Windows 7, Windows Vista oder Windows Server 2008 zu installieren, müssen Sie die Rechte für Ihren Microsoft Windows-Benutzeraccount erweitern. Unabhängig davon, ob Sie ein Benutzer mit Verwaltungsaufgaben oder ein Benutzer ohne Verwaltungsaufgaben sind, klicken Sie mit der rechten Maustaste auf die Datei `pmt.bat` und wählen Sie **Run as administrator** (Als Administrator ausführen) aus. Alternativ hierzu verwenden Sie den Befehl **runas** in der Befehlszeile. Beispiel:

```
runas /user:ADMINNAME /env pmt.bat
```

Benutzer ohne Verwaltungsaufgaben werden zur Eingabe des Administratorkennworts aufgefordert.

Bei einer Einzelserverumgebung muss ein eigenständiges Profil erstellt werden.

Führen Sie bei einer Network Deployment-Umgebung die folgenden Schritte aus:

1. Erstellen Sie das Deployment Manager-Profil vor der Erstellung anderer Profile. Wenn Sie vor der Installation von IBM Business Monitor (z. B. für WebSphere Application Server oder Process Server) ein Deployment Manager-Profil erstellt haben und dasselbe Deployment Manager-Profil für die Verwaltung der IBM

Business Monitor-Knoten verwenden möchten, müssen Sie das Profil mithilfe der von IBM Business Monitor bereitgestellten Vorlage erweitern.

2. Erstellen Sie für jeden Knoten, der zum Server-Cluster hinzugefügt werden soll, ein angepasstes Profil. Erweitern Sie alternativ für jeden Knoten, der hinzugefügt werden soll, ein bereits vorhandenes angepasstes Profil.

**Anmerkung:** Wenn der Datenbankserver mehrere installierte Versionen von DB2 oder mehrere DB2-Instanzen enthält, wird bei der Profilerstellung die DB2-Standardversion oder -instanz des Servers verwendet. Gehen Sie nach der Vorgehensweise 'Datenbank manuell installieren' vor, um zu steuern, welche DB2-Version oder -Instanz verwendet wird. So kann der Datenbankadministrator die Verwendung der korrekten Version oder Instanz sicherstellen.

Die JDBC-Unterstützung wird bei Verwendung einer Oracle-Datenbank durch die JDBC-Treiber von Oracle für JVM 1.6 bereitgestellt. Die JDBC-Treiberdatei `ojdbc6.jar` enthält den von Oracle unterstützten JDBC-Treiber zur Verwendung mit WebSphere Application Server Version 7. Die Datei `ojdbc6.jar` kann sowohl für Oracle 10g als auch für Oracle 11g verwendet werden. Weitere Informationen zu Mindesteinstellungen für Oracle erhalten Sie über den zugehörigen Link.

Standardmäßig verweist das Profile Management Tool auf die Datei `ojdbc6.jar`, die im Pfad `application_server-stammverzeichnis\jdbcdrivers\oracle` bereitsteht. Alternativ hierzu können Sie eine weitere JDBC-Treiberdatei `Oracle ojdbc6.jar` herunterladen und beim Ausführen des Profile Management Tool oder beim Ausführen des Befehls **manageprofiles** auf diese verweisen.

Wenn Sie eine SQL Server-Datenbank verwenden, erfolgt die Bereitstellung von JDBC-Unterstützung durch die JDBC-Treiber von SQL Server für JVM 1.6. IBM Business Monitor verwendet die Datei `sqljdbc4.jar` des Microsoft JDBC 2.0-Treibers. Standardmäßig verweist das Profile Management Tool auf die Datei `sqljdbc4.jar`, die im Pfad `application_server-stammverzeichnis\jdbcdrivers\SQLServer` bereitsteht. Alternativ hierzu können Sie eine weitere JDBC-Treiberdatei `sqljdbc4.jar` herunterladen und beim Ausführen des Profile Management Tool oder beim Ausführen des Befehls **manageprofiles** auf diese verweisen. Informationen zu den erforderlichen Mindesteinstellungen für SQL Server erhalten Sie über den zugehörigen Link.

## Eigenständige Profile erstellen

Wenn Sie während einer Einzelserverinstallation kein IBM Business Monitor-Profil erstellt haben, müssen Sie das Profil erstellen. Das Profil wird im Profilverzeichnis von WebSphere Application Server erstellt.

Bevor Sie diese Task ausführen, müssen Sie die folgenden Tasks abgeschlossen haben:

- Überprüfen, ob alle Hard- und Softwarevoraussetzungen erfüllt sind.
- IBM Business Monitor muss installiert sein.
- Anmelden beim System mit den erforderlichen Lese-, Schreib- und Ausführungsberechtigungen für das Profilverzeichnis von WebSphere Application Server.

### Windows





**Wichtig:** Um das Profile Management Tool unter Windows 7, Windows Vista oder Windows Server 2008 zu installieren, müssen Sie die Rechte für Ihren Microsoft Windows-Benutzeraccount erweitern. Unabhängig davon, ob Sie ein Benutzer mit

Verwaltungsaufgaben oder ein Benutzer ohne Verwaltungsaufgaben sind, klicken Sie mit der rechten Maustaste auf die Datei `pmt.bat` und wählen Sie **Run as administrator** (Als Administrator ausführen) aus. Alternativ hierzu verwenden Sie den Befehl **runas** in der Befehlszeile. Beispiel:

```
runas /user:ADMINNAME /env pmt.bat
```

Benutzer ohne Verwaltungsaufgaben werden zur Eingabe des Administratorkennworts aufgefordert.

Gehen Sie wie folgt vor, um mit dem Profile Management Tool ein eigenständiges Anwendungsserverprofil zu erstellen:

1. Öffnen Sie das Profile Management Tool mit einer der folgenden Methoden:
  - Klicken Sie in der Konsole 'Erste Schritte' von IBM Business Monitor auf **Profile Management Tool**.
  -  Klicken Sie auf **Start > Programme > IBM > Business Monitor 8.0 > Profile Management Tool**.
  -  Führen Sie die Datei `pmt.bat` aus, die sich in folgendem Verzeichnis befindet: `application_server-stammverzeichnis\bin\ProfileManagement`
  -   Wechseln Sie in das Verzeichnis `application_server-stammverzeichnis/bin/ProfileManagement` und geben Sie in einem Terminalfenster `./pmt.sh` ein.
2. Überprüfen Sie die Informationen in der Eingangsanzeige für das Profile Management Tool und klicken Sie dann auf **Launch Profile Management Tool** (Profile Management Tool starten).
3. Klicken Sie in der Anzeige 'Profiles' (Profile) auf **Erstellen**, um ein neues Profil zu erstellen.
4. Blenden Sie in der Anzeige 'Environment Selection' (Umgebungsauswahl) IBM Business Monitor ein, klicken Sie auf **Eigenständiger Monitor Server** (Eigenständiger Business Compass) und anschließend auf **Weiter**.

**Einschränkung:** Wenn die Anzeige der IBM Business Monitor-Option nicht möglich ist, kann dies darauf hindeuten, dass Sie Solaris im 64-Bit-Modus verwenden. In diesem Fall können Sie das Profile Management Tool nicht verwenden, sondern müssen den Befehl **manageprofiles** verwenden.

5. Wählen Sie in der Anzeige 'Profilerstellungsoptionen' den gewünschten Installationstyp aus und klicken Sie auf **Weiter**.
  - **Typische Profilerstellung** (Standard): Erstellt das IBM Business Monitor-Profil, das Standardkonfigurationseinstellungen verwendet. Das Profile Management Tool ordnet dem Profil, dem Knoten und der Zelle eindeutige Namen zu. Das Tool installiert außerdem die Administrationskonsole, installiert Standardanwendungen und ordnet eindeutige Portwerte zu. Sie haben während der Konfiguration die Option, die Verwaltungssicherheit zu aktivieren. Abhängig vom Betriebssystem und Ihren Benutzerberechtigungen kann das Tool einen Systemservice zur Ausführung von IBM Business Monitor erstellen
  - **Erweiterte Profilerstellung:** Erstellt das IBM Business Monitor-Profil mit Standardkonfigurationseinstellungen, oder ermöglicht die Auswahl eigener IBM Business Monitor-Komponenten. Sie können eigene Portwerte zuordnen. Sie können die Administrationskonsole implementieren, Musteranwendungen implementieren und eine Web-Server-Definition erstellen. Abhängig vom Betriebssystem und Ihren Benutzerberechtigungen können Sie auswählen, ob IBM Business Monitor als Systemservice ausgeführt werden soll. Sie

können die IBM Business Monitor-Modellkonfiguration ermitteln. Sie können eine Datenbankentwurfsdatei angeben oder eigene Werte für die Konfiguration der IBM Business Monitor-Datenbank zuordnen. Sie können die IBM Cognos BI-Konfiguration für die mehrdimensionale Datenanalyse auswählen.

6. Wenn Sie **Typische Profilerstellung** ausgewählt haben, dann fahren Sie mit Schritt 11: Anzeige 'Verwaltungssicherheit' fort.
7. Erweitert: Wählen Sie in der Anzeige 'Optionale Anwendungsimplementierung' die Optionen **Administrationskonsole implementieren** und **Standardanwendung implementieren** aus. Die Standardanwendung ist eine WebSphere Application Server-Anwendung. Klicken Sie auf **Weiter**.
8. Erweitert: Akzeptieren Sie in der Anzeige 'Profilname und -position' den Standardnamen und die Standardposition oder geben Sie einen Profilnamen und einen Verzeichnispfad für das Profil an, das die Dateien für die Laufzeitumgebung, wie beispielsweise Befehle, Konfigurationsdateien und Protokolldateien enthalten soll. Der Standardprofilname lautet WBMon01. Unter Windows ist C:\IBM\WebSphere\AppServer\profiles\WBMon01 ein typisches Profilverzeichnis.
9. Erweitert: Wenn Sie das Profil, das Sie erstellen, als Standardprofil benutzen möchten, wählen Sie **Dieses Profil als Standardprofil verwenden** aus. Klicken Sie auf **Weiter**.
10. Erweitert: Legen Sie einen Grad von Leistungsoptimierung fest, der für das Profil, das Sie erstellen, angemessen ist. Dieser Parameter ist ein Parameter von WebSphere Application Server. Weitere Informationen finden Sie unter Anwendungsserver mit Hilfe vordefinierter Optimierungsschablonen optimieren im WebSphere Application Server Information Center.
11. Erweitert: Geben Sie in der Anzeige 'Node and Host Names' (Knoten- und Hostnamen) neue Werte ein oder akzeptieren Sie die Standardwerte und klicken Sie anschließend auf **Weiter**.
  - Der Knotenname wird zu Verwaltungszwecken verwendet. Wenn es sich bei dem Knoten um einen eingebundenen Knoten handelt, muss der Knotenname innerhalb der Zelle eindeutig sein.
  - Der Servername ist ein logischer Name für den IBM Business Monitor-Server.
  - Der Hostname ist der DNS-Name (kurz oder lang) oder die IP-Adresse dieses Computers.
  - Der Zellename ist ein logischer Name für die Gruppe von Knoten, die durch diesen Deployment Manager verwaltet wird.
12. Wählen Sie in der Anzeige 'Verwaltungssicherheit' eine der folgenden Optionen aus und klicken Sie auf **Weiter**.
  - Wählen Sie zum Aktivieren der Sicherheit das Kontrollkästchen **Verwaltungssicherheit aktivieren** aus und geben Sie den Benutzernamen und das Kennwort ein.
  - Wählen Sie zum Inaktivieren der Sicherheit das Kontrollkästchen **Verwaltungssicherheit aktivieren** ab.


Informationen dazu, ob die Sicherheit aktiviert werden sollte, finden Sie im Abschnitt Verwaltungssicherheit im Information Center für WebSphere Application Server.

Wenn Sie **Typische Profilerstellung** ausgewählt haben, dann fahren Sie mit Schritt 21: Anzeige 'Datenbankkonfiguration' fort.

13. Erweitert: Wählen Sie in der Anzeige 'Security Certificate - Part 1' (Sicherheitszertifikat - Teil 1) aus, ob ein persönliches Standardzertifikat und ein Root-



Signing-Zertifikat erstellt oder aus Keystores importiert werden soll. Klicken Sie zur Erstellung neuer Zertifikate auf **Weiter**, um zur Verifizierungsseite zu gelangen. Um bereits vorhandene Zertifikate aus Keystores zu importieren, suchen Sie die Zertifikate und klicken Sie dann auf **Weiter**, um zur Verifizierungsseite zu gelangen.

14. Erweitert: Modifizieren Sie in der Anzeige 'Security Certificate - Part 2' (Sicherheitszertifikat - Teil 2) die Zertifikatsinformationen, um während der Profilerstellung neue Zertifikate zu erstellen. Stellen Sie beim Import bereits vorhandener Zertifikate aus Keystores mithilfe der Informationen sicher, dass die ausgewählten Zertifikate die erforderlichen Angaben enthalten. Wenn dies bei den ausgewählten Zertifikaten nicht der Fall ist, klicken Sie auf **Zurück**, um andere Zertifikate zu importieren. Es ist ratsam, das Keystore-Standardkennwort zu ändern, um die Sicherheit der Keystore-Dateien und SSL-Zertifikate zu gewährleisten. Weitere Informationen zur Sicherung der Kommunikation zwischen einem Server und einem Client finden Sie im Abschnitt Securing communications (Kommunikation schützen) im WebSphere Application Server Information Center.
15. Erweitert: Überprüfen Sie in der Anzeige 'Zuordnung von Port-Werten' die Ports, die während der Profilerstellung zugeordnet werden. Protokollieren Sie bei Bedarf diese Portwerte. Übernehmen Sie die angegebenen Werte oder geben Sie alternative Portnummern an und klicken Sie auf **Weiter**.
16.  Erweitert: Auf Windows-Systemen wird die Windows-Anzeige für die Dienstdefinition angezeigt. Die Option **Anwendungsserverprozess als Windows-Dienst ausführen** ist standardmäßig aktiviert und so konfiguriert, dass zur Anmeldung die Informationen zum Benutzerkonto des lokalen Systems verwendet werden. Übernehmen Sie die Windows-Standard Einstellungen für den Dienst oder inaktivieren Sie diese Option. Klicken Sie dann auf **Weiter**. Zum Ändern der Anmeldedaten für Windows-Dienste müssen Sie die Option **Mit dem angegebenen Benutzerkonto anmelden** auswählen und den Benutzernamen und das Kennwort für das alternative Benutzerkonto eingeben.  
Der **Starttyp** für den Windows-Dienst wird standardmäßig auf **Automatisch** gesetzt. Sie können den Wert für **Starttyp** optional auch in **Manuell** oder **Inaktiviert** ändern. Verwenden Sie hierzu die entsprechende Liste.  
Da Dienste unter Windows-Betriebssystemen globale Einstellungen darstellen, kann der Dienst von jedem Profil gestartet werden und es ist deshalb nur bedingt nachvollziehbar, welches Profil beispielsweise den Befehl „startServer“ abgesetzt hat. Zur Vermeidung potenzieller Anforderungskonflikte für Dienste zwischen verschiedenen Profilen sollten Sie die Option **Anwendungsserverprozess als Windows-Dienst ausführen** inaktivieren.

17. Erweitert: Wählen Sie in der Anzeige 'Web-Server-Definition' eine der folgenden Optionen aus:

- Wenn Sie eine Web-Server-Definition erstellen wollen, müssen Sie die Option **Web-Server-Definition erstellen** aktivieren. Übernehmen Sie die nachfolgenden Web-Server-Daten, die bereitgestellt werden oder nehmen Sie die erforderlichen Änderungen vor.

#### **Web-Server-Typ**

Zu den möglichen Optionen zählen IBM HTTP Server, Microsoft Internet Information Services, Sun Java System, Lotus Domino Web Server und Apache Web Server.

#### **Web-Server-Betriebssystem**

Verfügbare Optionen sind Windows, AIX, Solaris und z/OS.

### Name des Web-Servers

Geben Sie einen Namen für den Web-Server ein. Der Standardname lautet 'web-server1'.

### Hostname oder IP-Adresse des Web-Servers

Geben Sie den Hostnamen oder die IP-Adresse des Web-Servers ein. Der Name des lokalen Hosts wird standardmäßig angezeigt.

### Web-Server-Port (Standardwert 80)

Geben Sie die Portnummer des Web-Servers ein oder übernehmen Sie den Standardwert (80).

- Wenn Sie keine Web-Server-Definition erstellen wollen, müssen Sie das Kontrollkästchen **Web-Server-Definition erstellen** abwählen.

Web-Server-Definitionen definieren einen externen Web-Server für WebSphere Application Server und ermöglichen es Ihnen, Konfigurationsdateien für Web-Server-Plug-ins für den Web-Server und in einigen Fällen auch den Web-Server zu verwalten. Wenn Sie keinen Web-Server installiert haben oder diesen Arbeitsschritt zu einem späteren Zeitpunkt ausführen möchten, können Sie dies auf einfache Weise über die Administrationskonsole nachholen.

18. Erweitert: Wenn Sie das Erstellen einer Web-Server-Definition auf der vorherigen Anzeige ausgewählt haben, geben Sie einen Pfad für das Installationsverzeichnis des Web-Servers und für das Installationsverzeichnis des Web-Server-Plug-ins auf der Anzeige 'Web-Server-Definition (Teil 2)' ein.
19. Erweitert: Wählen Sie in der Anzeige IBM Business Process Manager-Monitormodelle die Option **IBM Business Monitor - globales Prozess-Monitormodell implementieren** aus, um die globale Prozess-Monitormodellanwendung zu installieren und zu konfigurieren. Mit diesem Modell können Sie BPEL- oder BPMN-Prozesse überwachen, die auf IBM Business Process Manager ausgeführt werden, ohne selbst Monitormodelle zu generieren oder zu implementieren.
20. Optional: Erweitert: Konfigurieren Sie die Datenbanken mit einer Entwurfsdatei.
  - a. Wählen Sie die Option **Datenbankentwurfsdatei zur Datenbankkonfiguration verwenden** aus, wenn Sie lieber eine Entwurfsdatei verwenden möchten, anstatt die Datenbankparameter in den folgenden Anzeigen anzugeben.
  - b. Klicken Sie auf **Durchsuchen**.
  - c. Geben Sie den vollständig qualifizierten Pfadnamen für die Entwurfsdatei an.
  - d. Klicken Sie auf **Next** (Weiter).
  - e. Wählen Sie die Option **Ausführung von Datenbankskripts verzögern (muss bei Verwendung einer fernen Datenbank ausgewählt werden)** aus, wenn Sie nicht möchten, dass während der Profilerstellung lokale Datenbanken automatisch erstellt und konfiguriert oder Tabellen in einer bereits vorhandenen Datenbank erstellt werden. Wenn dieses Kontrollkästchen nicht ausgewählt ist, werden lokale Datenbanken erstellt. Bei Auswahl dieser Option müssen die Skripts, die an dem im Feld des Ausgabeverzeichnis für Datenbankskripts auf dieser Seite angegebenen Standort gespeichert sind, durch Sie oder den Datenbankadministrator manuell ausgeführt werden. Wenn Sie die Skripts für Oracle erstellen, müssen Sie @DB\_PASSWORD@ durch das Kennwort für den Schemanamen ersetzen, bevor Sie die Skripts ausführen.

**Anmerkung:** Wenn der Datenbankserver mehrere installierte Versionen von DB2 oder mehrere DB2-Instanzen enthält, wird bei der Profilerstellung die DB2-Standardversion oder -instanz des Servers verwendet. Gehen Sie nach der Vorgehensweise 'Datenbank manuell installieren' vor, um zu steuern, welche DB2-Version oder -Instanz verwendet wird. So kann der Datenbankadministrator die Verwendung der korrekten Version oder Instanz sicherstellen.

Wenn Sie eine Entwurfsdatei angeben wollen, werden die Datenbankkonfigurationsanzeigen im Profile Management Tool übersprungen. Stattdessen wird die Position der Entwurfsdatei an die Befehlszeile übergeben, um die Datenbankkonfiguration abzuschließen. Weitere Informationen zur Verwendung einer Entwurfsdatei für die Datenbankkonfiguration finden Sie unter "Datenbankscrippts mit dem Datenbankentwurfstool erstellen oder konfigurieren".

21. Überprüfen Sie in der Anzeige 'Datenbankkonfiguration' Ihre Daten zur MONITOR-Datenbankkonfiguration:
    - a. Wählen Sie unter **Datenbankprodukt** Ihre Datenbank in der Liste aus.
    - b. Zur Angabe eines Zielverzeichnisses für generierte Scrippts müssen Sie die Option **Zielverzeichnis für generierte Scrippts überschreiben** aktivieren und im Feld **Ausgabeverzeichnis für Datenbankscrippts** den Pfad eingeben. (Das Standardverzeichnis lautet `monitor_stammverzeichnis\profiles\WBMon01\dbscripts\Monitor\plattform\.`)
    - c. Wählen Sie die Option **Ausführung von Datenbankscrippts verzögern (muss bei Verwendung einer fernen Datenbank ausgewählt werden)** aus, wenn Sie nicht möchten, dass während der Profilerstellung lokale Datenbanken automatisch erstellt und konfiguriert oder Tabellen in einer bereits vorhandenen Datenbank erstellt werden. Wenn dieses Kontrollkästchen nicht ausgewählt ist, werden lokale Datenbanken erstellt. Bei Auswahl dieser Option müssen die Scrippts, die an dem im Feld des Ausgabeverzeichnisses für Datenbankscrippts auf dieser Seite angegebenen Standort gespeichert sind, durch Sie oder den Datenbankadministrator manuell ausgeführt werden. Wenn Sie die Scrippts für Oracle erstellen, müssen Sie `@DB_PASSWORD@` durch das Kennwort für den Schemanamen ersetzen, bevor Sie die Scrippts ausführen.
- Anmerkung:** Wenn der Datenbankserver mehrere installierte Versionen von DB2 oder mehrere DB2-Instanzen enthält, wird bei der Profilerstellung die DB2-Standardversion oder -instanz des Servers verwendet. Gehen Sie nach der Vorgehensweise 'Datenbank manuell installieren' vor, um zu steuern, welche DB2-Version oder -Instanz verwendet wird. So kann der Datenbankadministrator die Verwendung der korrekten Version oder Instanz sicherstellen.
- d. Geben Sie im Feld **Datenbankname** den Datenbanknamen ein oder übernehmen Sie den Standardnamen (MONITOR).
  - e. Geben Sie im Feld **Schemaname** einen Schemanamen ein oder übernehmen Sie den Standardwert (MONITOR). Wenn Sie mit DB2 unter z/OS arbeiten, muss sich der Datenbankschemaname für IBM Business Monitor von dem allgemeinen Datenbankschemanamen von Process Server unterscheiden, um Kollisionen zwischen den Datenbankobjekten zu vermeiden.
  - f. Klicken Sie auf **Next** (Weiter).
22. Führen Sie in der Anzeige 'Datenbankkonfiguration (Teil 2)' die folgenden Schritte aus. Die Optionen variieren abhängig von dem Datenbankprodukt, das Sie auf der vorherigen Anzeige ausgewählt haben:

- a. Geben Sie im Feld **Benutzername zur Datenbankauthentifizierung** einen *Benutzernamen* ein. Dieser Wert stellt eine vorhandene Benutzer-ID mit Lese- und Schreibzugriff für die MONITOR-Tabellen dar.

**Anmerkung:** Bei Verwendung einer Oracle-Datenbank ist dieses Feld nicht editierbar.

- b. Geben Sie im Feld **Kennwort für die Datenbankauthentifizierung** ein *Kennwort* ein. Dieser Wert steht für das Kennwort, das der angegebenen Datenbankbenutzer-ID zugeordnet ist.
- c. Geben Sie im Feld **Kennwort bestätigen** ein *Kennwort* ein. Dieser Wert muss mit dem Wert für **Kennwort für die Datenbankauthentifizierung** übereinstimmen.
- d. Blättern Sie zu einem Pfad für die JDBC-Treiber-Klassenpfaddateien oder geben Sie einen solchen Pfad ein. Die JDBC-Treiber für DB2, Oracle und SQL Server befinden sich in `monitor_stammverzeichnis/jdbcdrivers`. Der Standardklassenpfad für den JDBC-Treiber ist so definiert, dass er die produktspezifischen Dateien in diesem Verzeichnis verwendet. Dabei wird der Datenbanktyp zugrunde gelegt, den Sie in der Anzeige 'Datenbankkonfiguration' ausgewählt haben. Alternativ hierzu können Sie auch auf **Durchsuchen** klicken, um einen Pfad zu den Klassenpfaddateien des JDBC-Treibers einzugeben.

- DB2-Datenbank: Das folgende Verzeichnis wird standardmäßig erstellt:  
`monitor_stammverzeichnis/jdbcdrivers/DB2`
- Oracle-Datenbank: Das folgende Verzeichnis wird standardmäßig erstellt:  
`monitor_stammverzeichnis/jdbcdrivers/Oracle`

Die JDBC-Treiberdatei `ojdbc6.jar` enthält den von Oracle unterstützten JDBC-Treiber zur Verwendung mit WebSphere Application Server Version 7. Die Datei `ojdbc6.jar` kann sowohl für Oracle 10g als auch für Oracle 11g verwendet werden. Weitere Informationen zu Mindesteinstellungen für Oracle erhalten Sie über den zugehörigen Link.

- SQL Server-Datenbank: Das folgende Verzeichnis wird standardmäßig erstellt:  
`monitor_stammverzeichnis/jdbcdrivers/SQLServer`

Die JDBC-Treiberdatei `sqljdbc4.jar` enthält den JDBC-Treiber für Microsoft SQL Server 2.0. Weitere Informationen zu Mindesteinstellungen für SQL Server erhalten Sie über den zugehörigen Link.

- e. Wählen Sie eine der folgenden Optionen für den Typ des JDBC-Treibers aus:
- Für Oracle-Datenbanken:
    - **OCI:** Der OCI-Treiber erfordert eine lokale Oracle-Clientinstallation.
    - **Thin:** Der Thin-Treiber verwendet Java für die Kommunikation mit der Datenbank und erfordert keinen Client auf dem lokalen System.
  - Bei DB2-Datenbanken werden Profile von IBM Business Monitor unter anderen Betriebssystemen als z/OS mit Treibern vom Typ 4 erstellt, während sie unter z/OS mit Treibern vom Typ 2 erstellt werden. Sie können den Typ nach der Profilerstellung ändern, indem Sie die Eigenschaften der Datenquelle in der Administrationskonsole bearbeiten. Ein Treiber vom Typ 2 ist ein nativer API-Treiber und erfordert die Installation der Datenbanksoftware oder eines Datenbankclients auf dem lokalen System. Ein Treiber des Typs 4 ist eine reine Java-Implementierung und

bietet in der Regel die beste Leistung. Für die MONITOR-Datenbank benötigen Sie auf dem lokalen System keine Datenbanksoftware und keine Clients.

- f. Geben Sie für **Hostname oder IP-Adresse des Datenbankservers** einen *Hostnamen* ein. Der Standardwert ist localhost oder der vollständig qualifizierte Name des lokalen Hosts, sofern dieser definiert ist, und sollte für eine Einzelserverinstallation verwendet werden. Wenn sich Ihre Datenbank auf einem fernen Server befindet, müssen Sie den vollständig qualifizierten Hostnamen oder die IP-Adresse eingeben.

**Anmerkung:** Verwenden Sie, außer in einer Einzelserverinstallation, *nicht* den Wert localhost, da die Cluster-Member von dem eigentlichen Hostnamen bzw. der eigentlichen IP-Adresse abhängig sind.




- g. Geben Sie für **Port des TCP/IP-Service oder Listener-Port der Datenbank** eine *Portnummer* ein. Dieser Wert steht für den Port, der dem TCP/IP-Service zugeordnet ist, oder für den Port, an dem die Datenbank empfangsbereit ist.
- h. Optional: Wenn Sie eine DB2-Datenbank unter z/OS verwenden, geben Sie für **Subsystemname** einen *Subsystemnamen* ein. Der Wert ist die Position der DB2 for z/OS-Datenbank. Es sind keine Leerzeichen im Namen zulässig.
- i. Wenn Sie Oracle oder SQL Server verwenden und die Datenbank automatisch erstellen möchten, geben Sie folgende Daten ein:
- Unter **Benutzername des Datenbankadministrators** den *Systembenutzernamen*. Dieser Wert ist der Name des Datenbankadministrators für Oracle oder SQL Server. Dieser Benutzer muss die Zugriffsberechtigungen zum Erstellen und Löschen von Datenbanken und Benutzern besitzen.
  - Im Feld **Kennwort** ein *Kennwort*. Dieser Wert ist das Kennwort des im vorherigen Feld angegebenen Systemadministrators.
  - Im Feld **Kennwort bestätigen** das *Kennwort*.
- j. Klicken Sie auf **Next** (Weiter). Wenn die MONITOR-Datenbank noch nicht erstellt wurde, wird eine Warnung angezeigt. Klicken Sie auf **Ja**, um fortzufahren. Sie können die Datenbank zu einem späteren Zeitpunkt erstellen.
23. Konfigurieren Sie in der IBM Cognos BI-Konfigurationsanzeige IBM Cognos BI für die mehrdimensionale Datenanalyse über Ihre Dashboards.
- Um IBM Cognos BI zu implementieren, müssen Sie auf **Neue Cognos-Serverkonfiguration erstellen** klicken und den Namen einer Datenbank angeben, die für den IBM Cognos BI-Content-Store verwendet werden soll. Der Standardname lautet COGNOSCS. Für Oracle ist der Datenbankname der Oracle-Servicename. Für Microsoft SQL Server darf der Name der Datenbank nicht mit dem Namen der MONITOR-Datenbank übereinstimmen. Geben Sie einen Datenbankbenutzernamen und das zugehörige Kennwort an. Wenn Sie für den Content-Store und die Monitor-Datenbank den gleichen Benutzernamen verwenden, dann müssen Sie auch das gleiche Kennwort benutzen. Da der Datenbankbenutzer, der zum Zugriff auf die Content-Store-Datenbank angegeben wird, über die Berechtigung zum Erstellen von Tabellen in der Datenbank verfügen muss, wird empfohlen, einen neuen Datenbankbenutzer nur für die Content-Store-Datenbank zu erstellen. Sie müssen außerdem den Benutzernamen des IBM Cognos BI-Administrators und das zugehörige Kennwort angeben.



**Anmerkung:** Der Benutzername und das Kennwort für die IBM Cognos BI-Content-Store-Datenbank werden in 'Cognos\_JDBC\_Alias' gespeichert. Dadurch ist es möglich, alle Berechtigungsnachweise für die Datenbank zentral zu verwalten. Wenn Sie den IBM Business Monitor IBM Cognos BI-Server starten, werden die aktuellen Werte an die IBM Cognos BI-Konfiguration übergeben, um IBM Cognos BI den Zugriff auf den Content-Store zu ermöglichen. Aufgrund dieser Integration können Sie den Benutzernamen und das Kennwort für den Content-Store mit der IBM Cognos BI-Konfigurationsanwendung nicht ändern.

- Wenn Sie eine vorhandene IBM Cognos BI-Version verwenden möchten, dann klicken Sie auf **Bestehende Cognos-Serverkonfiguration verwenden** und geben Sie die URI des externen Dispatchers des IBM Cognos BI-Servers an. Sie finden diese URI im IBM Cognos BI-Konfigurationsclient in **Lokale Konfiguration > Umgebung > Dispatcher-Einstellungen** (Beispiel: `http://my_host:my_port/p2pd/servlet/dispatch/ext`). Wenn die administrative Sicherheit auf dem IBM Cognos BI-Server aktiviert ist, müssen Sie auch den Benutzernamen und das Kennwort des IBM Cognos BI-Administrators angeben.

Der IBM Cognos BI-Server muss nicht verfügbar sein, um diesen Wert zu definieren. Der Server ist erforderlich, wenn Sie Monitormodelle installieren und die mehrdimensionale Analyse für diese Modelle ausführen wollen.

24. Überprüfen Sie die Informationen in der Anzeige 'Profilerstellung - Zusammenfassung'. Wenn Sie Änderungen durchführen möchten, dann klicken Sie auf **Zurück** und nehmen Sie die erforderlichen Änderungen vor.
25. Klicken Sie auf **Erstellen**, um das Profil zu erstellen.
26. Überprüfen Sie in der Anzeige 'Profilerstellung abgeschlossen' die Informationen zur abgeschlossenen Profilerstellung.
27. Optional: Rufen Sie die Konsole 'Erste Schritte' auf.
  -  Wählen Sie die Option **IBM Business Monitor-Erste Schritte starten** aus.
  -   Wechseln Sie zu `profil-stammverzeichnis/firststeps.wbm` und führen Sie den Befehl `firststeps.sh` aus.
28. Klicken Sie auf **Fertig stellen**, um das Profile Management Tool zu beenden.

Während der Profilerstellung definieren Sie Portwerte für alle erforderlichen Ports. Wenn Sie sich dazu entschließen, die Ports nach der Installation zu ändern, müssen Sie alle Portwerte erneut konfigurieren, damit IBM Business Monitor ordnungsgemäß ausgeführt werden kann.

## Deployment Manager-Profil erstellen

Sie müssen über ein Deployment Manager-Profil verfügen, um alle eingebundenen Server in einem Cluster zu verwalten. Wenn Sie eine Network Deployment-Umgebung einrichten, erstellen Sie zuerst dieses Profil.

Bevor Sie diese Task ausführen, müssen Sie die folgenden Tasks abgeschlossen haben:

- Überprüfen, ob alle Hard- und Softwarevoraussetzungen erfüllt sind.
- IBM Business Monitor muss installiert sein.
- Anmelden beim System mit den erforderlichen Lese-, Schreib- und Ausführungsberechtigungen für das Profilverzeichnis von WebSphere Application Server.
- Datenbank muss installiert sein





► Windows

**Wichtig:** Um das Profile Management Tool unter Windows 7, Windows Vista oder Windows Server 2008 zu installieren, müssen Sie die Rechte für Ihren Microsoft Windows-Benutzeraccount erweitern. Unabhängig davon, ob Sie ein Benutzer mit Verwaltungsaufgaben oder ein Benutzer ohne Verwaltungsaufgaben sind, klicken Sie mit der rechten Maustaste auf die Datei `pmt.bat` und wählen Sie **Run as administrator** (Als Administrator ausführen) aus. Alternativ hierzu verwenden Sie den Befehl **runas** in der Befehlszeile. Beispiel:

```
runas /user:ADMINNAME /env pmt.bat
```

Benutzer ohne Verwaltungsaufgaben werden zur Eingabe des Administratorkeywords aufgefordert.

Führen Sie die folgenden Schritte aus, um ein Deployment Manager-Profil mithilfe des Profile Management Tool zu erstellen:

1. Öffnen Sie das Profile Management Tool mit einer der folgenden Methoden:
  - Klicken Sie in der Konsole 'Erste Schritte' von IBM Business Monitor auf **Profile Management Tool**.
  -  Klicken Sie auf **Start > Programme > IBM > Business Monitor 8.0 > Profile Management Tool**.
  -  Führen Sie die Datei `pmt.bat` aus, die sich in folgendem Verzeichnis befindet: `application_server-stammverzeichnis\bin\ProfileManagement`
  -   Wechseln Sie in das Verzeichnis `application_server-stammverzeichnis/bin/ProfileManagement` und geben Sie in einem Terminalfenster `./pmt.sh` ein.
2. Überprüfen Sie die Informationen in der Eingangsanzeige für das Profile Management Tool und klicken Sie dann auf **Launch Profile Management Tool** (Profile Management Tool starten).
3. Klicken Sie in der Anzeige 'Profiles' (Profile) auf **Erstellen**, um ein neues Profil zu erstellen.
4. Blenden Sie in der Anzeige 'Environment Selection' (Umgebungsauswahl) IBM Business Monitor ein, klicken Sie auf **Monitor Server Deployment Manager** und anschließend auf **Weiter**.

**Einschränkung:** Wenn die Anzeige der IBM Business Monitor-Option nicht möglich ist, kann dies darauf hindeuten, dass Sie Solaris im 64-Bit-Modus verwenden. In diesem Fall können Sie das Profile Management Tool nicht verwenden, sondern müssen den Befehl **manageprofiles** verwenden.

5. Wählen Sie in der Anzeige 'Profileroptionsmöglichkeiten' den gewünschten Installationstyp aus und klicken Sie auf **Weiter**.
  - **Typische Profilerstellung** (Standard): Erstellt ein Deployment Manager-Profil, das Standardkonfigurationseinstellungen verwendet. Das Profile Management Tool ordnet dem Profil, dem Knoten, dem Host und der Zelle eindeutige Namen zu. Das Tool installiert außerdem die Administrationskonsole und ordnet eindeutige Portwerte zu. Sie haben während der Konfiguration die Option, die Verwaltungssicherheit zu aktivieren. Abhängig vom Betriebssystem und Ihren Benutzerberechtigungen kann das Tool einen Systemservice zur Ausführung des Deployment Managers erstellen. Sie können eigene Werte für die Konfiguration der IBM Business Monitor-Datenbank angeben.


- **Erweiterte Profilerstellung:** Erstellt einen Deployment Manager mit Standardkonfigurationseinstellungen. Sie können die Werte für den Host und die Zelle angeben, eigene Portwerte zuordnen und auswählen, ob die Administrationskonsole implementiert werden soll. Abhängig vom Betriebssystem und Ihren Benutzerberechtigungen haben Sie die Option, Deployment Manager als Systemservice auszuführen. Sie können eine Datenbankentwurfsdatei angeben oder eigene Werte für die Konfiguration der IBM Business Monitor-Datenbank zuordnen.
6. Wenn Sie **Typische Profilerstellung** ausgewählt haben, gehen Sie zu Schritt 10: Anzeige 'Verwaltungssicherheit'.
  7. Erweitert: Wählen Sie in der Anzeige 'Optionale Anwendungsimplementierung' die Option **Administrationskonsole implementieren** aus und klicken Sie auf **Weiter**.
  8. Erweitert: Akzeptieren Sie in der Anzeige 'Profilname und -position' den Standardnamen und die Standardposition oder geben Sie einen Profilnamen und einen Verzeichnispfad für das Profil an, das die Dateien für die Laufzeitumgebung, wie beispielsweise Befehle, Konfigurationsdateien und Protokolldateien enthalten soll. Der Standardprofilname lautet Dmgr01. Unter Windows ist C:\IBM\WebSphere\AppServer\profiles\Dmgr01 ein typisches Profilverzeichnis.
  9. Erweitert: Wenn Sie das Profil, das Sie erstellen, als Standardprofil benutzen möchten, wählen Sie **Dieses Profil als Standardprofil verwenden** aus. Klicken Sie auf **Next** (Weiter).
  10. Erweitert: Geben Sie in der Anzeige 'Node, Host, and Cell Names' (Knoten-, Host- und Zellennamen) neue Werte ein oder akzeptieren Sie die Standardwerte und klicken Sie anschließend auf **Weiter**.
    - Der Knotenname wird zu Verwaltungszwecken verwendet. Wenn es sich bei dem Knoten um einen eingebundenen Knoten handelt, muss der Knotenname innerhalb der Zelle eindeutig sein.
    - Der Hostname ist der DNS-Name (kurz oder lang) oder die IP-Adresse dieses Computers.
    - Der Zellename ist ein logischer Name für die Gruppe von Knoten, die durch diesen Deployment Manager verwaltet wird.
  11. Wählen Sie in der Anzeige 'Verwaltungssicherheit' eine der folgenden Optionen aus und klicken Sie auf **Weiter**.
    - Wählen Sie zum Aktivieren der Sicherheit das Kontrollkästchen **Verwaltungssicherheit aktivieren** aus und geben Sie den Benutzernamen und das Kennwort ein.
    - Wählen Sie zum Inaktivieren der Sicherheit das Kontrollkästchen **Verwaltungssicherheit aktivieren** ab.

Informationen dazu, ob die Sicherheit aktiviert werden sollte, finden Sie im Abschnitt Verwaltungssicherheit im Information Center für WebSphere Application Server.

Wenn Sie **Typische Profilerstellung** ausgewählt haben, dann fahren Sie mit Schritt 16: Anzeige 'Datenbankkonfiguration' fort.

12. Erweitert: Wählen Sie in der Anzeige 'Security Certificate - Part 1' (Sicherheitszertifikat - Teil 1) aus, ob ein persönliches Standardzertifikat und ein Root-Signing-Zertifikat erstellt oder aus Keystores importiert werden soll. Klicken Sie zur Erstellung neuer Zertifikate auf **Weiter**, um zur Verifizierungsseite zu gelangen. Um bereits vorhandene Zertifikate aus Keystores zu importieren, suchen Sie die Zertifikate und klicken Sie dann auf **Weiter**, um zur Verifizierungsseite zu gelangen.



13. Erweitert: Modifizieren Sie in der Anzeige 'Security Certificate - Part 2' (Sicherheitszertifikat - Teil 2) die Zertifikatsinformationen, um während der Profilerstellung neue Zertifikate zu erstellen. Stellen Sie beim Import bereits vorhandener Zertifikate aus Keystores mithilfe der Informationen sicher, dass die ausgewählten Zertifikate die erforderlichen Angaben enthalten. Wenn dies bei den ausgewählten Zertifikaten nicht der Fall ist, klicken Sie auf **Zurück**, um andere Zertifikate zu importieren. Es ist ratsam, das Keystore-Standardkennwort zu ändern, um die Sicherheit der Keystore-Dateien und SSL-Zertifikate zu gewährleisten. Weitere Informationen zur Sicherung der Kommunikation zwischen einem Server und einem Client finden Sie im Abschnitt Securing communications (Kommunikation schützen) im WebSphere Application Server Information Center.
14. Erweitert: Überprüfen Sie in der Anzeige 'Zuordnung von Port-Werten' die Ports, die während der Profilerstellung zugeordnet werden. Protokollieren Sie bei Bedarf diese Portwerte. Übernehmen Sie die angegebenen Werte oder geben Sie alternative Portnummern an und klicken Sie auf **Weiter**.
15.  Erweitert: Auf Windows-Systemen wird die Windows-Anzeige für die Dienstdefinition angezeigt. Die Option **Anwendungsserverprozess als Windows-Dienst ausführen** ist standardmäßig aktiviert und so konfiguriert, dass zur Anmeldung die Informationen zum Benutzerkonto des lokalen Systems verwendet werden. Übernehmen Sie die Windows-Standard Einstellungen für den Dienst oder inaktivieren Sie diese Option. Klicken Sie dann auf **Weiter**. Zum Ändern der Anmeldedaten für Windows-Dienste müssen Sie die Option **Mit dem angegebenen Benutzerkonto anmelden** auswählen und den Benutzernamen und das Kennwort für das alternative Benutzerkonto eingeben.  
Der **Starttyp** für den Windows-Dienst wird standardmäßig auf **Automatisch** gesetzt. Sie können den Wert für **Starttyp** optional auch in **Manuell** oder **Inaktiviert** ändern. Verwenden Sie hierzu die entsprechende Liste.  
Da Dienste unter Windows-Betriebssystemen globale Einstellungen darstellen, kann der Dienst von jedem Profil gestartet werden und es ist deshalb nur bedingt nachvollziehbar, welches Profil beispielsweise den Befehl „startServer“ abgesetzt hat. Zur Vermeidung potenzieller Anforderungskonflikte für Dienste zwischen verschiedenen Profilen sollten Sie die Option **Anwendungsserverprozess als Windows-Dienst ausführen** inaktivieren.
16. Optional: Erweitert: Konfigurieren Sie die Datenbanken mit einer Entwurfsdatei.
  - a. Wählen Sie die Option **Datenbankentwurfsdatei zur Datenbankkonfiguration verwenden** aus, wenn Sie lieber eine Entwurfsdatei verwenden möchten, anstatt die Datenbankparameter in den folgenden Anzeigen anzugeben.
  - b. Klicken Sie auf **Durchsuchen**.
  - c. Geben Sie den vollständig qualifizierten Pfadnamen für die Entwurfsdatei an.
  - d. Klicken Sie auf **Next** (Weiter).
  - e. Wählen Sie die Option **Ausführung von Datenbankskripts verzögern (muss bei Verwendung einer fernen Datenbank ausgewählt werden)** aus, wenn Sie nicht möchten, dass während der Profilerstellung lokale Datenbanken automatisch erstellt und konfiguriert oder Tabellen in einer bereits vorhandenen Datenbank erstellt werden. Wenn dieses Kontrollkästchen nicht ausgewählt ist, werden lokale Datenbanken erstellt. Bei Auswahl dieser Option müssen die Skripts, die an dem im Feld des Ausgabeverzeichnis für Datenbankskripts auf dieser Seite angegebenen Standort gespeichert sind, durch Sie oder den Datenbankadministrator manuell ausgeführt

werden. Wenn Sie die Scripts für Oracle erstellen, müssen Sie @DB\_PASSWORD@ durch das Kennwort für den Schemanamen ersetzen, bevor Sie die Scripts ausführen.

**Anmerkung:** Wenn der Datenbankserver mehrere installierte Versionen von DB2 oder mehrere DB2-Instanzen enthält, wird bei der Profilerstellung die DB2-Standardversion oder -instanz des Servers verwendet. Gehen Sie nach der Vorgehensweise 'Datenbank manuell installieren' vor, um zu steuern, welche DB2-Version oder -Instanz verwendet wird. So kann der Datenbankadministrator die Verwendung der korrekten Version oder Instanz sicherstellen.

Wenn Sie eine Entwurfsdatei angeben wollen, werden die Datenbankkonfigurationsanzeigen im Profile Management Tool übersprungen. Stattdessen wird die Position der Entwurfsdatei an die Befehlszeile übergeben, um die Datenbankkonfiguration abzuschließen. Weitere Informationen zur Verwendung einer Entwurfsdatei für die Datenbankkonfiguration finden Sie unter "Datenbankscrippts mit dem Datenbankentwurfstool erstellen oder konfigurieren".

17. Überprüfen Sie in der Anzeige 'Datenbankkonfiguration' Ihre Daten zur MONITOR-Datenbankkonfiguration:
  - a. Wählen Sie Ihr Datenbankprodukt in der Liste aus.
  - b. Zur Angabe eines Zielverzeichnisses für generierte Scripts müssen Sie die Option **Zielverzeichnis für generierte Scripts überschreiben** aktivieren und im Feld **Ausgabeverzeichnis für Datenbankscrippts** den Pfad eingeben. (Das Standardverzeichnis lautet `monitor_stammverzeichnis\profiles\WBMon01\dbscripts\Monitor\plattform\.`)
  - c. Wählen Sie die Option **Ausführung von Datenbankscrippts verzögern (muss bei Verwendung einer fernen Datenbank ausgewählt werden)** aus, wenn Sie nicht möchten, dass während der Profilerstellung oder -erweiterung eine lokale Datenbank automatisch erstellt und konfiguriert oder Tabellen in einer bereits vorhandenen Datenbank erstellt werden. Wenn dieses Kontrollkästchen nicht ausgewählt ist, wird eine lokale Datenbank erstellt. Bei Auswahl dieser Option müssen die Scripts, die an dem im Feld des Ausgabeverzeichnisses für Datenbankscrippts auf dieser Seite angegebenen Standort gespeichert sind, durch Sie oder den Datenbankadministrator manuell ausgeführt werden. Wenn Sie die Scripts für Oracle erstellen, müssen Sie @DB\_PASSWORD@ durch das Kennwort für den Schemanamen ersetzen, bevor Sie die Scripts ausführen.

**Anmerkung:** Wenn der Datenbankserver mehrere installierte Versionen von DB2 oder mehrere DB2-Instanzen enthält, wird bei der Profilerstellung die DB2-Standardversion oder -instanz des Servers verwendet. Gehen Sie nach der Vorgehensweise 'Datenbank manuell installieren' vor, um zu steuern, welche DB2-Version oder -Instanz verwendet wird. So kann der Datenbankadministrator die Verwendung der korrekten Version oder Instanz sicherstellen.

- d. Geben Sie im Feld **Datenbankname** den Datenbanknamen ein oder übernehmen Sie den Standardnamen (MONITOR).
- e. Geben Sie im Feld **Schemaname** einen Schemanamen ein oder übernehmen Sie den Standardwert (MONITOR). Wenn Sie mit DB2 unter z/OS arbeiten, muss sich der Datenbankschemaname für IBM Business Monitor von dem allgemeinen Datenbankschemanamen von Process Server unterscheiden, um Kollisionen zwischen den Datenbankobjekten zu vermeiden.
- f. Klicken Sie auf **Next** (Weiter).

18. Führen Sie auf der Anzeige 'Datenbankkonfiguration (Teil 2)' für die MONITOR-Datenbank die folgenden Schritte aus. Die Optionen variieren abhängig von dem Datenbankprodukt, das Sie auf der vorherigen Anzeige ausgewählt haben:

- a. Geben Sie im Feld **Benutzername zur Datenbankauthentifizierung** einen *Benutzernamen* ein. Dieser Wert stellt eine vorhanden Benutzer-ID mit Lese- und Schreibzugriff für die MONITOR-Tabellen dar.

**Anmerkung:** Bei Verwendung einer Oracle-Datenbank ist dieses Feld nicht editierbar.

- b. Geben Sie im Feld **Kennwort für die Datenbankauthentifizierung** ein *Kennwort* ein. Dieser Wert steht für das Kennwort, das der angegebenen Datenbankbenutzer-ID zugeordnet ist.
- c. Geben Sie im Feld **Kennwort bestätigen** ein *Kennwort* ein. Dieser Wert muss mit dem Wert für **Kennwort für die Datenbankauthentifizierung** übereinstimmen.
- d. Blättern Sie zu einem Pfad für die JDBC-Treiber-Klassenpfaddateien oder geben Sie einen solchen Pfad ein. Die JDBC-Treiber für DB2, Oracle und SQL Server befinden sich in `monitor_stammverzeichnis/jdbcdrivers`. Der Standardklassenpfad für den JDBC-Treiber ist so definiert, dass er die produktspezifischen Dateien in diesem Verzeichnis verwendet. Dabei wird der Datenbanktyp zugrunde gelegt, den Sie in der Anzeige 'Datenbankkonfiguration' ausgewählt haben. Alternativ hierzu können Sie auch auf **Durchsuchen** klicken, um einen Pfad zu den Klassenpfaddateien des JDBC-Treibers einzugeben.

- DB2-Datenbank: Das folgende Verzeichnis wird standardmäßig erstellt:  
`monitor_stammverzeichnis/jdbcdrivers/DB2`
- Oracle-Datenbank: Das folgende Verzeichnis wird standardmäßig erstellt:  
`monitor_stammverzeichnis/jdbcdrivers/Oracle`

Die JDBC-Treiberdatei `ojdbc6.jar` enthält den von Oracle unterstützten JDBC-Treiber zur Verwendung mit WebSphere Application Server Version 7. Die Datei `ojdbc6.jar` kann sowohl für Oracle 10g als auch für Oracle 11g verwendet werden. Weitere Informationen zu Mindesteinstellungen für Oracle erhalten Sie über den zugehörigen Link.

- SQL Server-Datenbank: Das folgende Verzeichnis wird standardmäßig erstellt:  
`monitor_stammverzeichnis/jdbcdrivers/SQLServer`

Die JDBC-Treiberdatei `sqljdbc4.jar` enthält den JDBC-Treiber für Microsoft SQL Server 2.0. Weitere Informationen zu Mindesteinstellungen für SQL Server erhalten Sie über den zugehörigen Link.

- e. Wählen Sie eine der folgenden Optionen für den Typ des JDBC-Treibers aus:
- Für Oracle-Datenbanken:
    - **OCI:** Der OCI-Treiber erfordert eine lokale Oracle-Clientinstallation.
    - **Thin:** Der Thin-Treiber verwendet Java für die Kommunikation mit der Datenbank und erfordert keinen Client auf dem lokalen System.
  - Bei DB2-Datenbanken werden Profile von IBM Business Monitor unter anderen Betriebssystemen als z/OS mit Treibern vom Typ 4 erstellt, während sie unter z/OS mit Treibern vom Typ 2 erstellt werden. Sie

können den Typ nach der Profilerstellung ändern, indem Sie die Eigenschaften der Datenquelle in der Administrationskonsole bearbeiten. Ein Treiber vom Typ 2 ist ein nativer API-Treiber und erfordert die Installation der Datenbanksoftware oder eines Datenbankclients auf dem lokalen System. Ein Treiber des Typs 4 ist eine reine Java-Implementierung und bietet in der Regel die beste Leistung. Für die MONITOR-Datenbank benötigen Sie auf dem lokalen System keine Datenbanksoftware und keine Clients.




- f. Geben Sie für **Hostname oder IP-Adresse des Datenbankservers** einen *Hostnamen* ein. Der Standardwert ist localhost oder der vollständig qualifizierte Name des lokalen Hosts, sofern dieser definiert ist, und sollte für eine Einzelserverinstallation verwendet werden. Wenn sich Ihre Datenbank auf einem fernen Server befindet, müssen Sie den vollständig qualifizierten Hostnamen oder die IP-Adresse eingeben.

**Anmerkung:** Verwenden Sie, außer in einer Einzelserverinstallation, *nicht* den Wert localhost, da die Cluster-Member von dem eigentlichen Hostnamen bzw. der eigentlichen IP-Adresse abhängig sind.

- g. Geben Sie für **Port des TCP/IP-Service oder Listener-Port der Datenbank** eine *Portnummer* ein. Dieser Wert steht für den Port, der dem TCP/IP-Service zugeordnet ist, oder für den Port, an dem die Datenbank empfangsbereit ist.
- h. Optional: Wenn Sie eine DB2-Datenbank unter z/OS verwenden, geben Sie für **Subsystemname** einen *Subsystemnamen* ein. Der Wert ist die Position der DB2 for z/OS-Datenbank. Es sind keine Leerzeichen im Namen zulässig.
- i. Wenn Sie Oracle oder SQL Server verwenden und die Datenbank automatisch erstellen möchten, geben Sie folgende Daten ein:
- Unter **Benutzername des Datenbankadministrators** den *Systembenutzernamen*. Dieser Wert ist der Name des Datenbankadministrators für Oracle oder SQL Server. Dieser Benutzer muss die Zugriffsberechtigungen zum Erstellen und Löschen von Datenbanken und Benutzern besitzen.
  - Im Feld **Kennwort** ein *Kennwort*. Dieser Wert ist das Kennwort des im vorherigen Feld angegebenen Systemadministrators.
  - Im Feld **Kennwort bestätigen** das *Kennwort*.
- j. Klicken Sie auf **Next** (Weiter). Wenn die MONITOR-Datenbank noch nicht erstellt wurde, wird eine Warnung angezeigt. Klicken Sie auf **Ja**, um fortzufahren. Sie können die Datenbank zu einem späteren Zeitpunkt erstellen.
19. Geben Sie in der Content-Store-Datenbankanzeige die notwendigen Informationen ein, um die IBM Cognos BI-Content-Store-Datenbank für mehrdimensionale Datenanalyse aus Ihren Dashboards zu erstellen, falls Sie nicht bereits eine vorhandene IBM Cognos Business Intelligence-Installation nutzen wollen.
- a. Klicken Sie auf **Neue Cognos-Content-Store-Datenbank erstellen**.
- b. Vergeben Sie einen Datenbanknamen, der für den IBM Cognos BI-Content-Store verwendet werden soll. Der Standardname lautet COGNOSCS. Für Oracle ist der Datenbankname der Oracle-Servicename. Für Microsoft SQL Server darf der Name der Datenbank nicht mit dem Namen der MONITOR-Datenbank übereinstimmen.
- c. Vergeben Sie einen Benutzernamen und ein Kennwort für die Datenbank und bestätigen Sie das Kennwort. Wenn Sie für den Content-Store und die Monitor-Datenbank den gleichen Benutzernamen verwenden, dann müssen Sie auch das gleiche Kennwort benutzen. Da dieser Benutzer die uneinge-

schränkte Zugriffsberechtigung benötigt, sollten Sie einen neuen Datenbankbenutzer erstellen, der ausschließlich für die Content-Store-Datenbank verwendet wird.

**Anmerkung:** Der Benutzername und das Kennwort für die IBM Cognos BI-Content-Store-Datenbank werden in 'Cognos\_JDBC\_Alias' gespeichert. Dadurch ist es möglich, alle Berechtigungsnachweise für die Datenbank zentral zu verwalten. Wenn Sie den IBM Business Monitor IBM Cognos BI-Server starten, werden die aktuellen Werte an die IBM Cognos BI-Konfiguration übergeben, um IBM Cognos BI den Zugriff auf den Content-Store zu ermöglichen. Aufgrund dieser Integration können Sie den Benutzernamen und das Kennwort für den Content-Store mit der IBM Cognos BI-Konfigurationsanwendung nicht ändern.

20. Überprüfen Sie die Informationen in der Anzeige 'Profilerstellung - Zusammenfassung'. Wenn Sie Änderungen durchführen möchten, dann klicken Sie auf **Zurück** und nehmen Sie die erforderlichen Änderungen vor.
21. Klicken Sie auf **Erstellen**, um das Profil zu erstellen.
22. Überprüfen Sie in der Anzeige 'Profilerstellung abgeschlossen' die Informationen zur abgeschlossenen Profilerstellung.
23. Optional: Rufen Sie die Konsole 'Erste Schritte' auf.
  -  Wählen Sie die Option **IBM Business Monitor-Erste Schritte starten** aus.
  -   Wechseln Sie zu `profil-stammverzeichnis/firststeps.wbm` und führen Sie den Befehl `firststeps.sh` aus.
24. Klicken Sie auf **Fertig stellen**, um das Profile Management Tool zu beenden.

Während der Profilerstellung definieren Sie Portwerte für alle erforderlichen Ports. Wenn Sie sich dazu entschließen, die Ports nach der Installation zu ändern, müssen Sie alle Portwerte erneut konfigurieren, damit IBM Business Monitor ordnungsgemäß ausgeführt werden kann.

## Deployment Manager-Profil erweitern

In einer Network Deployment-Umgebung müssen Sie über ein Deployment Manager-Profil verfügen. Sie können optional ein bestehendes Deployment Manager-Profil zu einem Deployment Manager-Profil für IBM Business Monitor erweitern und brauchen kein neues Profil zu erstellen.

Bevor Sie diese Task ausführen, müssen Sie die folgenden Tasks abgeschlossen haben:

- Überprüfen, ob alle Hard- und Softwarevoraussetzungen erfüllt sind.
- IBM Business Monitor muss installiert sein.
- Anmelden beim System mit den erforderlichen Lese-, Schreib- und Ausführungsberechtigungen für das Profilverzeichnis von WebSphere Application Server.
- Datenbank muss installiert sein

 **Windows**

**Wichtig:** Um das Profile Management Tool unter Windows 7, Windows Vista oder Windows Server 2008 zu installieren, müssen Sie die Rechte für Ihren Microsoft Windows-Benutzeraccount erweitern. Unabhängig davon, ob Sie ein Benutzer mit Verwaltungsaufgaben oder ein Benutzer ohne Verwaltungsaufgaben sind, klicken







Sie mit der rechten Maustaste auf die Datei `pmt.bat` und wählen Sie **Run as administrator** (Als Administrator ausführen) aus. Alternativ hierzu verwenden Sie den Befehl **runas** in der Befehlszeile. Beispiel:

```
runas /user:ADMINNAME /env pmt.bat
```

Benutzer ohne Verwaltungsaufgaben werden zur Eingabe des Administratorkennworts aufgefordert.

Sie können ein bestehendes WebSphere Application Server-, Process Server- oder WebSphere Enterprise Service Bus-Profil mit der IBM Business Monitor-Vorlage erweitern. Auf ähnliche Weise können Sie, wenn Sie WebSphere Application Server installiert und das Profil für IBM Business Monitor erweitert haben, das Profil mit Process Server oder WebSphere Enterprise Service Bus erweitern.

Führen Sie die folgenden Schritte aus, um mit dem Profile Management Tool ein bereits vorhandenes Deployment Manager-Profil zu erweitern:

1. Öffnen Sie das Profile Management Tool mit einer der folgenden Methoden:
  - Klicken Sie in der Konsole 'Erste Schritte' von IBM Business Monitor auf **Profile Management Tool**.
  -  Klicken Sie auf **Start > Programme > IBM > Business Monitor 8.0 > Profile Management Tool**.
  -  Führen Sie die Datei `pmt.bat` aus, die sich in folgendem Verzeichnis befindet: `application_server-stammverzeichnis\bin\ProfileManagement`
  -   Wechseln Sie in das Verzeichnis `application_server-stammverzeichnis/bin/ProfileManagement` und geben Sie in einem Terminalfenster `./pmt.sh` ein.
2. Überprüfen Sie die Informationen in der Eingangsanzeige für das Profile Management Tool und klicken Sie dann auf **Launch Profile Management Tool** (Profile Management Tool starten).
3. Wählen Sie in der Anzeige 'Profiles' (Profile) ein Profil aus der Liste aus und klicken Sie auf **Erweitern**, um das bereits vorhandene Profil zu erweitern. (Sie können die bereits durchgeführten Erweiterungen anzeigen, indem Sie ein Profil einblenden.) Sie müssen ein bereits vorhandenes Deployment Manager-Profil auswählen, das als Deployment Manager-Profil für IBM Business Monitor erweitert werden soll.

**Einschränkung:** Wenn die Anzeige der IBM Business Monitor-Option nicht möglich ist, kann dies darauf hindeuten, dass Sie Solaris im 64-Bit-Modus verwenden. In diesem Fall können Sie das Profile Management Tool nicht verwenden, sondern müssen den Befehl **manageprofiles** verwenden.

4. Klicken Sie in der Anzeige 'Erweiterungsauswahl' in der Liste auf **Monitor Server Deployment Manager** und dann auf **Weiter**.
5. Klicken Sie in der Anzeige 'Profilerweiterungsoptionen' auf **Erweiterte Profilerweiterung** und dann auf **Weiter**. Wenn Sie auf die Option für die **Typische Profilerweiterung** klicken, werden nicht alle Anzeigen angezeigt.
6. Optional: Wenn für das Profil, das Sie erweitern wollen, die Sicherheit aktiviert ist, müssen Sie in der Anzeige für die Verwaltungssicherheit die folgenden Schritte ausführen:
  - a. Geben Sie im Feld **Benutzername** einen *Benutzernamen* ein.
  - b. Geben Sie im Feld **Kennwort** ein *Kennwort* ein.
  - c. Geben Sie im Feld **Kennwort bestätigen** ein *Kennwort* ein.
  - d. Klicken Sie auf **Next** (Weiter).

7. Optional: Erweitert: Konfigurieren Sie die Datenbanken mit einer Entwurfsdatei.
  - a. Wählen Sie die Option **Datenbankentwurfsdatei zur Datenbankkonfiguration verwenden** aus, wenn Sie lieber eine Entwurfsdatei verwenden möchten, anstatt die Datenbankparameter in den folgenden Anzeigen anzugeben.
  - b. Klicken Sie auf **Durchsuchen**.
  - c. Geben Sie den vollständig qualifizierten Pfadnamen für die Entwurfsdatei an.
  - d. Klicken Sie auf **Next** (Weiter).
  - e. Wählen Sie die Option **Ausführung von Datenbankskripts verzögern (muss bei Verwendung einer fernen Datenbank ausgewählt werden)** aus, wenn Sie nicht möchten, dass während der Profilerstellung lokale Datenbanken automatisch erstellt und konfiguriert oder Tabellen in einer bereits vorhandenen Datenbank erstellt werden. Wenn dieses Kontrollkästchen nicht ausgewählt ist, werden lokale Datenbanken erstellt. Bei Auswahl dieser Option müssen die Skripts, die an dem im Feld des Ausgabeverzeichnis für Datenbankskripts auf dieser Seite angegebenen Standort gespeichert sind, durch Sie oder den Datenbankadministrator manuell ausgeführt werden. Wenn Sie die Skripts für Oracle erstellen, müssen Sie @DB\_PASSWORD@ durch das Kennwort für den Schemanamen ersetzen, bevor Sie die Skripts ausführen.

**Anmerkung:** Wenn der Datenbankserver mehrere installierte Versionen von DB2 oder mehrere DB2-Instanzen enthält, wird bei der Profilerstellung die DB2-Standardversion oder -instanz des Servers verwendet. Gehen Sie nach der Vorgehensweise 'Datenbank manuell installieren' vor, um zu steuern, welche DB2-Version oder -Instanz verwendet wird. So kann der Datenbankadministrator die Verwendung der korrekten Version oder Instanz sicherstellen.

Wenn Sie eine Entwurfsdatei angeben wollen, werden die Datenbankkonfigurationsanzeigen im Profile Management Tool übersprungen. Stattdessen wird die Position der Entwurfsdatei an die Befehlszeile übergeben, um die Datenbankkonfiguration abzuschließen. Weitere Informationen zur Verwendung einer Entwurfsdatei für die Datenbankkonfiguration finden Sie unter "Datenbankskripts mit dem Datenbankentwurfstool erstellen oder konfigurieren".

8. Überprüfen Sie in der Anzeige 'Datenbankkonfiguration' Ihre Daten zur MONITOR-Datenbankkonfiguration:
  - a. Wählen Sie Ihr Datenbankprodukt in der Liste aus.
  - b. Zur Angabe eines Zielverzeichnisses für generierte Skripts müssen Sie die Option **Zielverzeichnis für generierte Skripts überschreiben** aktivieren und im Feld **Ausgabeverzeichnis für Datenbankskripts** den Pfad eingeben. (Das Standardverzeichnis lautet `monitor_stammverzeichnis\profiles\WBMon01\dbscripts\Monitor\plattform\.`)
  - c. Wählen Sie die Option **Ausführung von Datenbankskripts verzögern (muss bei Verwendung einer fernen Datenbank ausgewählt werden)** aus, wenn Sie nicht möchten, dass während der Profilerstellung oder -erweiterung eine lokale Datenbank automatisch erstellt und konfiguriert oder Tabellen in einer bereits vorhandenen Datenbank erstellt werden. Wenn dieses Kontrollkästchen nicht ausgewählt ist, wird eine lokale Datenbank erstellt. Bei Auswahl dieser Option müssen die Skripts, die an dem im Feld des Ausgabeverzeichnisses für Datenbankskripts auf dieser Seite angegebenen Standort gespeichert sind, durch Sie oder den Datenbankadministrator



manuell ausgeführt werden. Wenn Sie die Scripts für Oracle erstellen, müssen Sie @DB\_PASSWORD@ durch das Kennwort für den Schemanamen ersetzen, bevor Sie die Scripts ausführen.

**Anmerkung:** Wenn der Datenbankserver mehrere installierte Versionen von DB2 oder mehrere DB2-Instanzen enthält, wird bei der Profilerstellung die DB2-Standardversion oder -instanz des Servers verwendet. Gehen Sie nach der Vorgehensweise 'Datenbank manuell installieren' vor, um zu steuern, welche DB2-Version oder -Instanz verwendet wird. So kann der Datenbankadministrator die Verwendung der korrekten Version oder Instanz sicherstellen.

- d. Geben Sie im Feld **Datenbankname** den Datenbanknamen ein oder übernehmen Sie den Standardnamen (MONITOR).
  - e. Geben Sie im Feld **Schemaname** einen Schemanamen ein oder übernehmen Sie den Standardwert (MONITOR). Wenn Sie mit DB2 unter z/OS arbeiten, muss sich der Datenbankschemaname für IBM Business Monitor von dem allgemeinen Datenbankschemanamen von Process Server unterscheiden, um Kollisionen zwischen den Datenbankobjekten zu vermeiden.
  - f. Klicken Sie auf **Next** (Weiter).
9. Führen Sie auf der Anzeige 'Datenbankkonfiguration (Teil 2)' für die MONITOR-Datenbank die folgenden Schritte aus. Die Optionen variieren abhängig von dem Datenbankprodukt, das Sie auf der vorherigen Anzeige ausgewählt haben:
- a. Geben Sie im Feld **Benutzername zur Datenbankauthentifizierung** einen *Benutzernamen* ein. Dieser Wert stellt eine vorhandene Benutzer-ID mit Lese- und Schreibzugriff für die MONITOR-Tabellen dar.

**Anmerkung:** Bei Verwendung einer Oracle-Datenbank ist dieses Feld nicht editierbar.

- b. Geben Sie im Feld **Kennwort für die Datenbankauthentifizierung** ein *Kennwort* ein. Dieser Wert steht für das Kennwort, das der angegebenen Datenbankbenutzer-ID zugeordnet ist.
- c. Geben Sie im Feld **Kennwort bestätigen** ein *Kennwort* ein. Dieser Wert muss mit dem Wert für **Kennwort für die Datenbankauthentifizierung** übereinstimmen.
- d. Blättern Sie zu einem Pfad für die JDBC-Treiber-Klassenpfaddateien oder geben Sie einen solchen Pfad ein. Die JDBC-Treiber für DB2, Oracle und SQL Server befinden sich in `monitor_stammverzeichnis/jdbcdrivers`. Der Standardklassenpfad für den JDBC-Treiber ist so definiert, dass er die produktspezifischen Dateien in diesem Verzeichnis verwendet. Dabei wird der Datenbanktyp zugrunde gelegt, den Sie in der Anzeige 'Datenbankkonfiguration' ausgewählt haben. Alternativ hierzu können Sie auch auf **Durchsuchen** klicken, um einen Pfad zu den Klassenpfaddateien des JDBC-Treibers einzugeben.
  - DB2-Datenbank: Das folgende Verzeichnis wird standardmäßig erstellt:  
`monitor_stammverzeichnis/jdbcdrivers/DB2`
  - Oracle-Datenbank: Das folgende Verzeichnis wird standardmäßig erstellt:  
`monitor_stammverzeichnis/jdbcdrivers/Oracle`

Die JDBC-Treiberdatei `ojdbc6.jar` enthält den von Oracle unterstützten JDBC-Treiber zur Verwendung mit WebSphere Application Server Version 7. Die Datei `ojdbc6.jar` kann sowohl für Oracle 10g als auch für

Oracle 11g verwendet werden. Weitere Informationen zu Mindesteinstellungen für Oracle erhalten Sie über den zugehörigen Link.

- SQL Server-Datenbank: Das folgende Verzeichnis wird standardmäßig erstellt:

monitor\_stammverzeichnis/jdbcdrivers/SQLServer

Die JDBC-Treiberdatei sqljdbc4.jar enthält den JDBC-Treiber für Microsoft SQL Server 2.0. Weitere Informationen zu Mindesteinstellungen für SQL Server erhalten Sie über den zugehörigen Link.




- e. Wählen Sie eine der folgenden Optionen für den Typ des JDBC-Treibers aus:
- Für Oracle-Datenbanken:
    - **OCI**: Der OCI-Treiber erfordert eine lokale Oracle-Clientinstallation.
    - **Thin**: Der Thin-Treiber verwendet Java für die Kommunikation mit der Datenbank und erfordert keinen Client auf dem lokalen System.
  - Bei DB2-Datenbanken werden Profile von IBM Business Monitor unter anderen Betriebssystemen als z/OS mit Treibern vom Typ 4 erstellt, während sie unter z/OS mit Treibern vom Typ 2 erstellt werden. Sie können den Typ nach der Profilerstellung ändern, indem Sie die Eigenschaften der Datenquelle in der Administrationskonsole bearbeiten. Ein Treiber vom Typ 2 ist ein nativer API-Treiber und erfordert die Installation der Datenbanksoftware oder eines Datenbankclients auf dem lokalen System. Ein Treiber des Typs 4 ist eine reine Java-Implementierung und bietet in der Regel die beste Leistung. Für die MONITOR-Datenbank benötigen Sie auf dem lokalen System keine Datenbanksoftware und keine Clients.
- f. Geben Sie für **Hostname oder IP-Adresse des Datenbankservers** einen *Hostnamen* ein. Der Standardwert ist localhost oder der vollständig qualifizierte Name des lokalen Hosts, sofern dieser definiert ist, und sollte für eine Einzelserverinstallation verwendet werden. Wenn sich Ihre Datenbank auf einem fernen Server befindet, müssen Sie den vollständig qualifizierten Hostnamen oder die IP-Adresse eingeben.

**Anmerkung:** Verwenden Sie, außer in einer Einzelserverinstallation, *nicht* den Wert localhost, da die Cluster-Member von dem eigentlichen Hostnamen bzw. der eigentlichen IP-Adresse abhängig sind.

- g. Geben Sie für **Port des TCP/IP-Service oder Listener-Port der Datenbank** eine *Portnummer* ein. Dieser Wert steht für den Port, der dem TCP/IP-Service zugeordnet ist, oder für den Port, an dem die Datenbank empfangsbereit ist.
- h. Optional: Wenn Sie eine DB2-Datenbank unter z/OS verwenden, geben Sie für **Subsystemname** einen *Subsystemnamen* ein. Der Wert ist die Position der DB2 for z/OS-Datenbank. Es sind keine Leerzeichen im Namen zulässig.
- i. Wenn Sie Oracle oder SQL Server verwenden und die Datenbank automatisch erstellen möchten, geben Sie folgende Daten ein:
- Unter **Benutzername des Datenbankadministrators** den *Systembenutzernamen*. Dieser Wert ist der Name des Datenbankadministrators für Oracle oder SQL Server. Dieser Benutzer muss die Zugriffsberechtigungen zum Erstellen und Löschen von Datenbanken und Benutzern besitzen.
  - Im Feld **Kennwort** ein *Kennwort*. Dieser Wert ist das Kennwort des im vorherigen Feld angegebenen Systemadministrators.

- Im Feld **Kennwort bestätigen** das *Kennwort*.
  - j. Klicken Sie auf **Next** (Weiter). Wenn die MONITOR-Datenbank noch nicht erstellt wurde, wird eine Warnung angezeigt. Klicken Sie auf **Ja**, um fortzufahren. Sie können die Datenbank zu einem späteren Zeitpunkt erstellen.
10. Geben Sie in der Content-Store-Datenbankanzeige die notwendigen Informationen ein, um die IBM Cognos BI-Content-Store-Datenbank für mehrdimensionale Datenanalyse aus Ihren Dashboards zu erstellen, falls Sie nicht bereits eine vorhandene IBM Cognos Business Intelligence-Installation nutzen wollen.
- a. Klicken Sie auf **Neue Cognos-Content-Store-Datenbank erstellen**.
  - b. Vergeben Sie einen Datenbanknamen, der für den IBM Cognos BI-Content-Store verwendet werden soll. Der Standardname lautet COGNOSCS. Für Oracle ist der Datenbankname der Oracle-Servicename. Für Microsoft SQL Server darf der Name der Datenbank nicht mit dem Namen der MONITOR-Datenbank übereinstimmen.
  - c. Vergeben Sie einen Benutzernamen und ein Kennwort für die Datenbank und bestätigen Sie das Kennwort. Wenn Sie für den Content-Store und die Monitor-Datenbank den gleichen Benutzernamen verwenden, dann müssen Sie auch das gleiche Kennwort benutzen. Da dieser Benutzer die uneingeschränkte Zugriffsberechtigung benötigt, sollten Sie einen neuen Datenbankbenutzer erstellen, der ausschließlich für die Content-Store-Datenbank verwendet wird.

**Anmerkung:** Der Benutzername und das Kennwort für die IBM Cognos BI-Content-Store-Datenbank werden in 'Cognos\_JDBC\_Alias' gespeichert. Dadurch ist es möglich, alle Berechtigungsnachweise für die Datenbank zentral zu verwalten. Wenn Sie den IBM Business Monitor IBM Cognos BI-Server starten, werden die aktuellen Werte an die IBM Cognos BI-Konfiguration übergeben, um IBM Cognos BI den Zugriff auf den Content-Store zu ermöglichen. Aufgrund dieser Integration können Sie den Benutzernamen und das Kennwort für den Content-Store mit der IBM Cognos BI-Konfigurationsanwendung nicht ändern.

11. Überprüfen Sie die Informationen in der Anzeige 'Profilerweiterung - Zusammenfassung'. Wenn Sie Änderungen durchführen möchten, dann klicken Sie auf **Zurück** und nehmen Sie die erforderlichen Änderungen vor.
12. Klicken Sie auf **Erweitern**, um das Profil zu erweitern.
13. Überprüfen Sie in der Anzeige 'Profilerweiterung abgeschlossen' die Informationen zur abgeschlossenen Profilerweiterung.
14. Optional: Rufen Sie die Konsole 'Erste Schritte' auf.
  -  Wählen Sie die Option **IBM Business Monitor-Erste Schritte starten** aus.
  -   Wechseln Sie zu `profil-stammverzeichnis/firststeps.wbm` und führen Sie den Befehl `firststeps.sh` aus.
15. Klicken Sie auf **Fertig stellen**, um das Profile Management Tool zu beenden.

Während der Profilerstellung definieren Sie Portwerte für alle erforderlichen Ports. Wenn Sie sich dazu entschließen, die Ports nach der Installation zu ändern, müssen Sie alle Portwerte erneut konfigurieren, damit IBM Business Monitor ordnungsgemäß ausgeführt werden kann.

## Angepasste Profile für Knoten erstellen

Bei einer Netzimplementierung müssen Sie ein angepasstes Profil für jeden Knoten erstellen, den Sie zum Server-Cluster von IBM Business Monitor hinzufügen wollen. Das Profil wird im Profilverzeichnis von WebSphere Application Server erstellt.

Bevor Sie diese Task ausführen, müssen Sie die folgenden Tasks abgeschlossen haben:

- Überprüfen, ob alle Hard- und Softwarevoraussetzungen erfüllt sind.
- IBM Business Monitor muss installiert sein.
- Anmelden beim System mit den erforderlichen Lese-, Schreib- und Ausführungsberechtigungen für das Profilverzeichnis von WebSphere Application Server.
- Sicherstellen, dass der Deployment Manager aktiv ist.

**Tipp:** Wenn Sie die Sicherheit auf den Knoten aktivieren möchten, sollten Sie die Sicherheit konfigurieren, bevor Sie mit dem Erstellen der angepassten Knoten fortfahren. Ausführliche Informationen zum Konfigurieren der Sicherheit können Sie über den unten angegebenen Link aufrufen.

### Windows

**Wichtig:** Um das Profile Management Tool unter Windows 7, Windows Vista oder Windows Server 2008 zu installieren, müssen Sie die Rechte für Ihren Microsoft Windows-Benutzeraccount erweitern. Unabhängig davon, ob Sie ein Benutzer mit Verwaltungsaufgaben oder ein Benutzer ohne Verwaltungsaufgaben sind, klicken Sie mit der rechten Maustaste auf die Datei pmt.bat und wählen Sie **Run as administrator** (Als Administrator ausführen) aus. Alternativ hierzu verwenden Sie den Befehl **runas** in der Befehlszeile. Beispiel:

```
runas /user:ADMINNAME /env pmt.bat
```

Benutzer ohne Verwaltungsaufgaben werden zur Eingabe des Administratorkeywords aufgefordert.

Führen Sie die folgenden Schritte aus, um mit dem Profile Management Tool ein angepasstes Profil für jedes Cluster-Member zu erstellen:

1. Öffnen Sie das Profile Management Tool mit einer der folgenden Methoden:
  - Klicken Sie in der Konsole 'Erste Schritte' von IBM Business Monitor auf **Profile Management Tool**.
  - **Windows** Klicken Sie auf **Start > Programme > IBM > Business Monitor 8.0 > Profile Management Tool**.
  - **Windows** Führen Sie die Datei pmt.bat aus, die sich in folgendem Verzeichnis befindet: application\_server-stammverzeichnis\bin\ProfileManagement
  - **Linux** **UNIX** Wechseln Sie in das Verzeichnis application\_server-stammverzeichnis/bin/ProfileManagement und geben Sie in einem Terminalfenster ./pmt.sh ein.
2. Überprüfen Sie die Informationen in der Eingangsanzeige für das Profile Management Tool und klicken Sie dann auf **Launch Profile Management Tool** (Profile Management Tool starten).
3. Klicken Sie in der Anzeige 'Profiles' (Profile) auf **Erstellen**, um ein neues Profil zu erstellen.




4. Blenden Sie in der Anzeige 'Environment Selection' (Umgebungsauswahl) IBM Business Monitor ein, klicken Sie auf **Angepasstes Monitor Server-Profil** (Angepasstes Business Compass-Profil) und anschließend auf **Weiter**. Das Erstellen eines angepassten Profils ermöglicht Ihnen die Erstellung von Servern und Clustern während der Einrichtung Ihrer Umgebung.

**Einschränkung:** Wenn die Anzeige der IBM Business Monitor-Option nicht möglich ist, kann dies darauf hindeuten, dass Sie Solaris im 64-Bit-Modus verwenden. In diesem Fall können Sie das Profile Management Tool nicht verwenden, sondern müssen den Befehl **manageprofiles** verwenden.

5. Wählen Sie in der Anzeige 'Profilerstellungsoptionen' den gewünschten Installationstyp aus und klicken Sie auf **Weiter**.
  - **Typische Profilerstellung** (Standard): Erstellt ein angepasstes Profil, das Standardkonfigurationseinstellungen verwendet. Das Profile Management Tool ordnet dem Profil, dem Knoten und dem Host eindeutige Namen zu. Der Knoten wird in einen vorhandenen Deployment Manager eingebunden.
  - **Erweiterte Profilerstellung:** Erstellt ein angepasstes Profil mit Standardkonfigurationseinstellungen. Sie können die Werte für die Position des Profils sowie die Namen für das Profil, den Knoten und den Host angeben. Der Knoten wird in einen vorhandenen Deployment Manager eingebunden.
6. Wenn Sie **Typische Profilerstellung** ausgewählt haben, dann fahren Sie mit Schritt 10: Anzeige 'Einbindung' fort.
7. Erweitert: Akzeptieren Sie in der Anzeige 'Profilname und -position' den Standardnamen und die Standardposition oder geben Sie einen Profilnamen und einen Verzeichnispfad für das Profil an, das die Dateien für die Laufzeitumgebung, wie beispielsweise Befehle, Konfigurationsdateien und Protokolldateien enthalten soll. Der Standardprofilname lautet Custom01. Unter Windows ist C:\IBM\WebSphere\AppServer\profiles\Custom01 ein typisches Profilverzeichnis.
8. Optional: Erweitert: Wenn Sie das Profil, das Sie erstellen, als Standardprofil benutzen möchten, wählen Sie **Dieses Profil als Standardprofil verwenden** aus. Klicken Sie auf **Next** (Weiter).
9. Erweitert: Geben Sie in der Anzeige 'Node and Host Names' (Knoten- und Hostnamen) neue Werte ein oder akzeptieren Sie die Standardwerte und klicken Sie anschließend auf **Weiter**.
  - Der Knotenname wird zu Verwaltungszwecken verwendet. Wenn es sich bei dem Knoten um einen eingebundenen Knoten handelt, muss der Knotenname innerhalb der Zelle eindeutig sein.
  - Der Hostname ist der DNS-Name (kurz oder lang) oder die IP-Adresse dieses Computers.
10. Führen Sie in der Anzeige 'Einbindung' die folgenden Schritte aus, um das Profil des Deployment Managers zu identifizieren, das verwendet werden soll:

**Anmerkung:** Sie können den Knoten zu einem späteren Zeitpunkt einbinden (mithilfe von 'add\_node'), indem Sie die Option **Diesen Knoten später einbinden** auswählen. Wenn Sie diese Option auswählen, werden alle Felder inaktiviert. Ein Vorteil der späteren Einbindung besteht darin, dass ein Profil ggf. nicht zweimal erstellt werden muss. Wenn der Knoten während der Profilerstellung eingebunden wurde und dieser Vorgang aus bestimmten Gründen fehlgeschlagen ist (z. B. dadurch, dass die Systemuhr des Knotens nicht mit der Systemuhr des Deployment Managers synchronisiert war), dann müssen Sie das Profil erneut erstellen, um seine Gültigkeit sicherzustellen. Wenn Sie

den Knoten zu einem späteren Zeitpunkt einbinden, dann ermöglicht Ihnen dies eine detailliertere Steuerung der Einbindungsprozedur.

- a. Geben Sie für **Hostname oder IP-Adresse des Deployment Managers** einen *Hostnamen* ein. Dieser Wert stellt den vollständig qualifizierten Hostnamen oder die IP-Adresse des Servers dar, auf dem das Profil des Deployment Managers erstellt wurde.
  - b. Geben Sie im Feld **SOAP-Portnummer des Deployment Managers** eine *Portnummer* ein. Der Standardwert lautet 8879.
  - c. Optional: Wenn die Verwaltungssicherheit auf dem Deployment Manager aktiviert ist, müssen Sie im Feld **Benutzername** einen *Benutzernamen* eingeben. Als Benutzername muss der Name eines bereits vorhandenen WebSphere Application Server-Benutzers für den Deployment Manager angegeben werden. Dieser Wert wird für die Authentifizierung beim Deployment Manager benötigt.
  - d. Optional: Wenn die Verwaltungssicherheit auf dem Deployment Manager aktiviert ist, müssen Sie im Feld **Kennwort** ein *Kennwort* eingeben. Dieses Kennwort muss für den Benutzernamen gelten, der in *benutzername* angegeben wurde.
  - e. Klicken Sie auf **Weiter**.
11. Wenn Sie **Typische Profilerstellung** ausgewählt haben, dann fahren Sie mit Schritt 15: Anzeige 'Profilerstellung - Zusammenfassung' fort.
  12. Erweitert: Überprüfen Sie in der Anzeige 'Zuordnung von Port-Werten' die Ports, die während der Profilerstellung zugeordnet werden. Protokollieren Sie bei Bedarf diese Portwerte. Übernehmen Sie die angegebenen Werte oder geben Sie alternative Portnummern an und klicken Sie auf **Weiter**.
  13. Erweitert: Gehen Sie in der Anzeige 'Datenbankkonfiguration' wie folgt vor:
    - a. Wählen Sie Ihr Datenbankprodukt in der Dropdown-Liste aus.
    - b. Geben Sie im Feld **Position (Verzeichnis) der Dateien im Klassenpfad des JDBC-Treibers** das Verzeichnis ein, in dem die JDBC-Klassenpfaddateien gespeichert sind, oder durchsuchen Sie die Verzeichnisstruktur nach diesem Verzeichnis.
    - c. Klicken Sie auf **Next** (Weiter).
  14. Überprüfen Sie die Informationen in der Anzeige 'Profilerstellung - Zusammenfassung'. Wenn Sie Änderungen durchführen möchten, dann klicken Sie auf **Zurück** und nehmen Sie die erforderlichen Änderungen vor.
  15. Klicken Sie auf **Erstellen**, um das Profil zu erstellen.
  16. Überprüfen Sie in der Anzeige 'Profilerstellung abgeschlossen' die Informationen zur abgeschlossenen Profilerstellung.
  17. Optional: Rufen Sie die Konsole 'Erste Schritte' auf.
    -  Wählen Sie die Option **IBM Business Monitor-Erste Schritte starten** aus.
    -   Wechseln Sie zu `profil-stammverzeichnis/firststeps.wbm` und führen Sie den Befehl `firststeps.sh` aus.
  18. Klicken Sie auf **Fertig stellen**, um das Profile Management Tool zu beenden.

Während der Profilerstellung definieren Sie Portwerte für alle erforderlichen Ports. Wenn Sie sich dazu entschließen, die Ports nach der Installation zu ändern, müssen Sie alle Portwerte erneut konfigurieren, damit IBM Business Monitor ordnungsgemäß ausgeführt werden kann.



## Angepasste Profile für Knoten erweitern

Bei einer Netzimplementierung benötigen Sie ein angepasstes Profil für jeden Knoten, den Sie zum Server-Cluster von IBM Business Monitor hinzufügen wollen. Sie können optional ein bestehendes Deployment Manager-Profil für jeden Knoten erweitern und brauchen kein neues Profil zu erstellen.

Bevor Sie diese Task ausführen, müssen Sie die folgenden Tasks abgeschlossen haben:

- Überprüfen, ob alle Hard- und Softwarevoraussetzungen erfüllt sind.
- IBM Business Monitor muss installiert sein.
- Anmelden beim System mit den erforderlichen Lese-, Schreib- und Ausführungsberechtigungen für das Profilverzeichnis von WebSphere Application Server.
- Sicherstellen, dass der Deployment Manager aktiv ist.

### Windows

**Wichtig:** Um das Profile Management Tool unter Windows 7, Windows Vista oder Windows Server 2008 zu installieren, müssen Sie die Rechte für Ihren Microsoft Windows-Benutzeraccount erweitern. Unabhängig davon, ob Sie ein Benutzer mit Verwaltungsaufgaben oder ein Benutzer ohne Verwaltungsaufgaben sind, klicken Sie mit der rechten Maustaste auf die Datei `pmt.bat` und wählen Sie **Run as administrator** (Als Administrator ausführen) aus. Alternativ hierzu verwenden Sie den Befehl `runas` in der Befehlszeile. Beispiel:

```
runas /user:ADMINNAME /env pmt.bat
```

Benutzer ohne Verwaltungsaufgaben werden zur Eingabe des Administratorkennworts aufgefordert.

Führen Sie die folgenden Schritte aus, um mit dem Profile Management Tool ein Profil für jedes Cluster-Member zu erweitern:




1. Öffnen Sie das Profile Management Tool mit einer der folgenden Methoden:
  - Klicken Sie in der Konsole 'Erste Schritte' von IBM Business Monitor auf **Profile Management Tool**.
  -  Klicken Sie auf **Start > Programme > IBM > Business Monitor 8.0 > Profile Management Tool**.
  -  Führen Sie die Datei `pmt.bat` aus, die sich in folgendem Verzeichnis befindet: `application_server-stammverzeichnis\bin\ProfileManagement`
  -   Wechseln Sie in das Verzeichnis `application_server-stammverzeichnis/bin/ProfileManagement` und geben Sie in einem Terminalfenster `./pmt.sh` ein.
2. Überprüfen Sie die Informationen in der Eingangsanzeige für das Profile Management Tool und klicken Sie dann auf **Launch Profile Management Tool** (Profile Management Tool starten).
3. Wählen Sie in der Anzeige 'Profiles' (Profile) ein Profil aus der Liste aus und klicken Sie auf **Erweitern**, um das bereits vorhandene Profil zu erweitern. (Sie können die bereits durchgeführten Erweiterungen anzeigen, indem Sie ein Profil einblenden.) Sie müssen ein bereits vorhandenes angepasstes Profil auswählen, das als angepasstes Profil für IBM Business Monitor erweitert werden soll. Ein angepasstes Profil ermöglicht Ihnen die Erstellung von Servern und Clustern während der Einrichtung Ihrer Umgebung.



**Einschränkung:** Wenn die Anzeige der IBM Business Monitor-Option nicht möglich ist, kann dies darauf hindeuten, dass Sie Solaris im 64-Bit-Modus verwenden. In diesem Fall können Sie das Profile Management Tool nicht verwenden, sondern müssen den Befehl **manageprofiles** verwenden.

4. Klicken Sie in der Anzeige 'Erweiterungsauswahl' in der Liste auf **Angepass-tes Monitor Server-Profil** und dann auf **Weiter**.
5. Klicken Sie in der Anzeige 'Profilerweiterungsoptionen' auf **Erweiterte Profi-lerweiterung** und dann auf **Weiter**. Wenn Sie auf die Option für die **Typische Profilerweiterung** klicken, werden nicht alle Anzeigen angezeigt.
6. Wenn die Anzeige 'Einbindung' geöffnet wird, führen Sie die folgenden Schrit-te aus, um das Profil des Deployment Managers zu identifizieren, das verwen-det werden soll:

**Anmerkung:** Wenn das Profil nicht vorher eingebunden wurde, wird diese Anzeige nicht geöffnet.

- a. Geben Sie für **Hostname oder IP-Adresse des Deployment Managers** ei-nen *Hostnamen* ein. Dieser Wert stellt den vollständig qualifizierten Hostna-men oder die IP-Adresse des Servers dar, auf dem das Profil des Deploy-ment Managers erstellt wurde.
  - b. Geben Sie im Feld **SOAP-Portnummer des Deployment Managers** eine *Portnummer* ein. Der Standardwert lautet 8879.
  - c. Optional: Wenn die Verwaltungssicherheit auf dem Deployment Manager aktiviert ist, müssen Sie im Feld **Benutzername** einen *Benutzernamen* einge-ben. Als Benutzername muss der Name eines bereits vorhandenen Web-Sphere Application Server-Benutzers für den Deployment Manager angege-ben werden. Dieser Wert wird für die Authentifizierung beim Deployment Manager benötigt.
  - d. Optional: Wenn die Verwaltungssicherheit auf dem Deployment Manager aktiviert ist, müssen Sie im Feld **Kennwort** ein *Kennwort* eingeben. Dieses Kennwort muss für den Benutzernamen gelten, der in *benutzername* ange-gaben wurde.
  - e. Klicken Sie auf **Weiter**.
7. Führen Sie in der Anzeige 'Datenbankkonfiguration' die folgenden Schritte aus:
    - a. Wählen Sie Ihr Datenbankprodukt in der Liste aus.
    - b. Geben Sie im Feld **Position (Verzeichnis) der Dateien im Klassenpfad des JDBC-Treibers** das Verzeichnis ein, in dem die JDBC-Klassenpfaddateien gespeichert sind, oder durchsuchen Sie die Verzeichnisstruktur nach die-sem Verzeichnis.
    - c. Klicken Sie auf **Next** (Weiter).
  8. Klicken Sie auf **Erweitern**, um das Profil zu erweitern.
  9. Überprüfen Sie in der Anzeige 'Profilerweiterung abgeschlossen' die Informati-onen zur abgeschlossenen Profilerweiterung.
  10. Optional: Rufen Sie die Konsole 'Erste Schritte' auf.
    -  Wählen Sie die Option **IBM Business Monitor-Erste Schritte star-ten** aus.
    -   Wechseln Sie zu `profil-stammverzeichnis/firststeps.wbm` und führen Sie den Befehl `firststeps.sh` aus.
  11. Klicken Sie auf **Fertig stellen**, um das Profile Management Tool zu beenden.

Während der Profilerstellung definieren Sie Portwerte für alle erforderlichen Ports. Wenn Sie sich dazu entschließen, die Ports nach der Installation zu ändern, müssen Sie alle Portwerte erneut konfigurieren, damit IBM Business Monitor ordnungsgemäß ausgeführt werden kann.

---

## Profile mit dem Befehl 'manageprofiles' erstellen und erweitern

Statt mit dem Profile Management Tool können Sie Profile mit dem Befehl **manageprofiles** über die Befehlszeile erstellen. Bei Verwendung der 64-Bit-Version von IBM Business Monitor müssen Sie den Befehl **manageprofiles** verwenden, weil das Profile Management Tool nicht unterstützt wird. Wenn Sie mit z/OS arbeiten, dann lesen Sie die Informationen im Abschnitt zum Erstellen allgemeiner Konfigurationen für IBM Business Monitor for z/OS.

**Wichtig:** Der Befehl **manageprofiles** unterstützt keine Profilerweiterung mit dem Parameter `profileTemplate` für Zellen in einem anderen Paket.

Sehen Sie sich die verfügbaren Parameter sorgfältig an, bevor Sie Ihr Profil erstellen oder erweitern. Ein Profil kann nach seiner Erstellung oder Erweiterung nicht mehr auf einfache Weise geändert werden.

Bevor Sie diese Task ausführen, müssen Sie die folgenden Tasks abgeschlossen haben:

- Überprüfen, ob alle Hard- und Softwarevoraussetzungen erfüllt sind.
- IBM Business Monitor muss installiert sein.
- Anmelden beim System mit den erforderlichen Lese-, Schreib- und Ausführungsberechtigungen für das Profilverzeichnis von WebSphere Application Server.

Die JDBC-Unterstützung wird bei Verwendung einer Oracle-Datenbank durch die JDBC-Treiber von Oracle für JVM 1.6 bereitgestellt. Die JDBC-Treiberdatei `ojdbc6.jar` enthält den von Oracle unterstützten JDBC-Treiber zur Verwendung mit WebSphere Application Server Version 7. Die Datei `ojdbc6.jar` kann sowohl für Oracle 10g als auch für Oracle 11g verwendet werden. Weitere Informationen zu Mindesteinstellungen für Oracle erhalten Sie über den zugehörigen Link.

Standardmäßig verweist das Profile Management Tool auf die Datei `ojdbc6.jar`, die im Pfad `application_server-stammverzeichnis\jdbcdrivers\oracle` bereitsteht. Alternativ hierzu können Sie eine weitere JDBC-Treiberdatei Oracle `ojdbc6.jar` herunterladen und beim Ausführen des Profile Management Tool oder beim Ausführen des Befehls **manageprofiles** auf diese verweisen.

Wenn Sie eine SQL Server-Datenbank verwenden, erfolgt die Bereitstellung von JDBC-Unterstützung durch die JDBC-Treiber von SQL Server für JVM 1.6. IBM Business Monitor verwendet die Datei `sqljdbc4.jar` des Microsoft JDBC 2.0-Treibers. Standardmäßig verweist das Profile Management Tool auf die Datei `sqljdbc4.jar`, die im Pfad `application_server-stammverzeichnis\jdbcdrivers\SQLServer` bereitsteht. Alternativ hierzu können Sie eine weitere JDBC-Treiberdatei `sqljdbc4.jar` herunterladen und beim Ausführen des Profile Management Tool oder beim Ausführen des Befehls **manageprofiles** auf diese verweisen. Informationen zu den erforderlichen Mindesteinstellungen für SQL Server erhalten Sie über den zugehörigen Link.

► Windows

**Wichtig:** Zum Installieren oder Ausführen des Befehls **manageprofiles** unter Windows 7, Windows Vista oder Windows Server 2008 müssen Sie die Rechte für Ihren Microsoft Windows-Benutzeraccount mit dem Befehl **runas** erweitern. Vergessen Sie nicht, den Befehl **manageprofiles** und alle Parameter in Anführungszeichen einzuschließen. Beispiel:

```
runas /env /user:MyAdminName "manageprofiles.bat -create -profileName WBMON01 -templatePath C:/WAS
```

Benutzer ohne Verwaltungsaufgaben werden zur Eingabe des Administratorkennworts aufgefordert.

Bei einer Einzelserverumgebung muss ein eigenständiges Profil erstellt werden.

Führen Sie bei einer Network Deployment-Umgebung die folgenden Schritte aus:

1. Erstellen Sie das Deployment Manager-Profil vor der Erstellung anderer Profile. Wenn Sie vor der Installation von IBM Business Monitor (z. B. für WebSphere Application Server oder Process Server) ein Deployment Manager-Profil erstellt haben und dasselbe Deployment Manager-Profil für die Verwaltung der IBM Business Monitor-Knoten verwenden möchten, müssen Sie das Profil mithilfe der von IBM Business Monitor bereitgestellten Vorlage erweitern.
2. Erstellen Sie für jeden Knoten, der zum Server-Cluster hinzugefügt werden soll, ein angepasstes Profil. Erweitern Sie alternativ für jeden Knoten, der hinzugefügt werden soll, ein bereits vorhandenes angepasstes Profil.

**Anmerkung:** Wenn der Datenbankserver mehrere installierte Versionen von DB2 oder mehrere DB2-Instanzen enthält, wird bei der Profilerstellung die DB2-Standardversion oder -instanz des Servers verwendet. Gehen Sie nach der Vorgehensweise 'Datenbank manuell installieren' vor, um zu steuern, welche DB2-Version oder -Instanz verwendet wird. So kann der Datenbankadministrator die Verwendung der korrekten Version oder Instanz sicherstellen.

Gehen Sie wie folgt vor, um ein Profil manuell zu erstellen:

1. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zu folgendem Verzeichnis:  
application\_server-stammverzeichnis/bin
2. Führen Sie den Befehl `manageprofiles.bat` bzw. `manageprofiles.sh` mit den erforderlichen Parametern aus. Auf den Referenzseiten finden Sie Details zu den Parametern für jeden einzelnen Profiltyp.



---

## Kapitel 7. Installation überprüfen

Nachdem Sie IBM Business Monitor installiert und ein Profil erstellt haben, können Sie optional über die Konsole 'Erste Schritte' überprüfen, ob das Produkt ordnungsgemäß installiert wurde.

1. Rufen Sie die Konsole 'Erste Schritte' auf.
  - Öffnen Sie ein Befehlsfenster. Wechseln Sie in das Verzeichnis `profil-stammverzeichnis/firststeps.wbm` und führen Sie den Befehl `firststeps.sh` aus.
  - Wählen Sie in der Anzeige **Profilerstellung abgeschlossen** die Option **IBM Business Monitor-Erste Schritte starten** aus.
  - Rufen Sie **Start > Alle Programme > IBM > Business Monitor 7.5 > Profiles > *profilname* > First Steps** auf.
  - Gehen Sie zu `profil-stammverzeichnis\firststeps.wbm` und führen Sie den Befehl `firststeps.bat` aus.

**Wichtig:** Um die Einführung (First Steps) unter Windows 7, Windows Vista oder Windows Server 2008 zu installieren, müssen Sie die Rechte Ihres Microsoft Windows Benutzeraccounts erweitern, indem Sie mit der rechten Maustaste auf `firststeps.bat` klicken und **Run as administrator** (Als Administrator ausführen) auswählen. Dies ist sowohl für Administratoren als auch für Benutzer ohne Administratorrechte erforderlich.

2. Wählen Sie in der Konsole 'Erste Schritte' die Option zur Ausführung eines Installationsprüftests aus.
3. Prüfen Sie die Ergebnisse.

Wenn Sie die Sicherheit für IBM Business Monitor aktiviert haben, müssen Sie nach der Installation zum Einrichten von Benutzern eine Benutzer-ID und ein Kennwort für den Authentifizierungsalias 'MonitorBusAuth' angeben. Weitere Informationen hierzu finden Sie in Berechtigungsnachweise in einer gesicherten Umgebung mit IBM Business Monitor angeben.

Neben dem Installationsprüftest stellt die Konsole 'Erste Schritte' auch Optionen zum Ausführen des Profile Management Tool, zum Öffnen der Administrationskonsole von WebSphere Application Server und zum Öffnen von Business Space zur Verfügung.

Auf einem Linux- oder UNIX-System muss möglicherweise das Eigentumsrecht vom Rootbenutzer auf einen anderen Benutzer übertragen werden. Sie können diese Task in IBM Business Monitor genauso wie in WebSphere Application Server oder Process Server ausführen. Weitere Informationen hierzu erhalten Sie über die unten aufgeführten zugehörigen Links.

Wenn Sie ein neues IBM Business Monitor-Profil erstellen oder ein vorhandenes Profil mit IBM Business Monitor erweitern und dabei der Ergebniscode `INSTCONFPARTIALSUCCESS` oder `INSTCONFFAILED` ausgegeben wird, beachten Sie die Tabelle im zugehörigen Linkverweis.



---

## Kapitel 8. Portnummern ermitteln

Zur Ermittlung der Portnummer für Webschnittstellen wie Business Space und die portletbasierten Dashboards überprüfen Sie die Konfiguration in der Administrationskonsole von WebSphere Application Server.

In einer Network Deployment-Umgebung wird aus Sicherheitsgründen und zum Zwecke des Lastausgleichs normalerweise ein Proxy-Server oder ein HTTP-Server verwendet. Eingehende HTTP-Anforderungen werden nicht direkt an ein bestimmtes Cluster-Member, sondern an einen Proxy-Server weitergeleitet, der die Anforderungen auf mehrere Cluster-Member verteilen kann, die die Verarbeitung durchführen. In diesem Fall benötigen Sie den Hostnamen und eine Portnummer des Proxy-Servers oder Web-Servers, der die Anforderung an einen Cluster-Member weiterleitet.

- Führen Sie die folgenden Schritte aus, um die Portnummern für einen Anwendungsserver zu ermitteln:
  1. Wählen Sie in der Administrationskonsole von WebSphere Application Server die Optionen **Server > Servertypen > WebSphere Application Server** aus.
  2. Wählen Sie den Namen des entsprechenden Servers oder Cluster-Members aus (z. B. **server1**).
  3. Klicken Sie unter 'Übertragungen' auf **Ports**.

Die Portnummer für Webschnittstellen wie Business Space und die portletbasierten Dashboards wird in einer Umgebung mit Sicherheit als `WC_defaulthost_secure` und in einer Umgebung ohne Sicherheit als `WC_defaulthost` aufgeführt. Ferner werden auf dieser Seite die Portnummern für den Bootstrap-Port, den SOAP-Connector-Port und weitere Ports angezeigt, die Sie beim Arbeiten mit IBM Business Monitor möglicherweise eingeben müssen.

- Führen Sie die folgenden Schritte aus, um die Portnummern für einen Proxy-Server zu ermitteln:
  1. Wählen Sie in der Administrationskonsole von WebSphere Application Server die Optionen **Server > Servertypen > WebSphere-Proxy-Server** aus.
  2. Wählen Sie den Namen des entsprechenden Servers aus (z. B. **proxy**).
  3. Klicken Sie unter 'Übertragungen' auf **Ports**.

Die Portnummer für Webschnittstellen wie Business Space und die portletbasierten Dashboards wird in einer Umgebung mit Sicherheit als `PROXY_HTTPS_ADDRESS` und in einer Umgebung ohne Sicherheit als `PROXY_HTTP_ADDRESS` aufgeführt. Ferner werden auf dieser Seite die Portnummern für den Bootstrap-Port, den SOAP-Connector-Port und weitere Ports angezeigt, die Sie beim Arbeiten mit IBM Business Monitor möglicherweise eingeben müssen.

Die Webmodule werden auf einem virtuellen Host implementiert (Standardname: `defaulthost`). Virtuelle Hosts werden in der Administrationskonsole konfiguriert. Klicken Sie dazu auf **Umgebung > Virtuelle Hosts**. Der für ein Webmodul ausgewählte virtuelle Host muss den HTTP- oder HTTPS-Port angeben, der von dem Server (oder Cluster-Member) verwendet wird, auf dem die Webmodule implementiert werden. Zusätzlich sollten alle IBM Business Monitor-Webmodule denselben virtuellen Host verwenden. Es gibt Webmodule in den meisten IBM Business Monitor-, Business Space- und REST-Anwendungen (EAR-Dateien).





---

## Kapitel 9. Umgebung konfigurieren

Nach der Installation von IBM Business Monitor in einer Network Deployment-Topologie müssen Sie weitere Konfigurationstasks ausführen, um die erforderlichen Ressourcen zu installieren und Ihre Umgebung vollständig auf die Überwachung vorzubereiten.

Bei der Erstellung eines eigenständigen Profils für IBM Business Monitor werden die erforderlichen Ressourcen automatisch als Teil des Profilerstellungsprozesses erstellt. Sie können die Administrationskonsole zur Überprüfung des Status oder zur erneuten Implementierung einer manuell entfernten Komponente verwenden, doch in der Regel sind die Konfigurationstasks in diesem Abschnitt ausschließlich zur Netzimplementierung erforderlich.

---

### Implementierungsumgebung mit einem Muster erstellen

Mit dem Konfigurationsassistenten für Implementierungsumgebungen können Sie den oder die Cluster erstellen und alle erforderlichen Komponenten für eine IBM Business Monitor Network Deployment-Topologie konfigurieren.

Bevor Sie Cluster erstellen und die IBM Business Monitor-Komponenten konfigurieren, müssen Sie die folgenden Aufgaben ausgeführt haben:

- Sie haben IBM Business Monitor installiert.
- Sie haben das Deployment Manager-Profil für IBM Business Monitor erstellt oder ein vorhandenes Deployment Manager-Profil mit IBM Business Monitor erweitert.
- Sie haben die Monitor-Datenbank erstellt.
- Sie haben den Deployment Manager gestartet.
- Sie haben mindestens ein angepasstes IBM Business Monitor-Profil erstellt und eingebunden oder ein vorhandenes angepasstes Profil mit IBM Business Monitor erweitert.
- Sie haben das angepasste Profil bzw. die Profile gestartet.

Stellen Sie vor dem Starten des Konfigurationsprozesses sicher, dass Sie Änderungen am Knoten automatisch synchronisieren (klicken Sie in der Administrationskonsole auf **Systemverwaltung > Konsoleinstellungen** und wählen Sie **Änderungen mit Knoten synchronisieren**) aus. Andernfalls müssen Sie die Änderungen nach jedem Hauptschritt manuell synchronisieren.

Es sind zwei Muster für IBM Business Monitor verfügbar: das Einzelclustermuster und das Vier-Cluster-Muster für fernes Messaging, Fernunterstützung und Webanwendungen.

Einer der optionalen Schritte im Konfigurationsassistenten für Implementierungsumgebungen ist das Importieren eines Datenbankentwurfsskizzen. Im Datenbankentwurfsskizzen wird die Datenbankkonfiguration für die ausgewählten Implementierungsumgebungsfunktionen definiert. Die Informationen des Entwurfsskizzen werden auf der Datenbankseite des Assistenten wiedergegeben. IBM Business Monitor enthält ein über eine Antwortdatei gesteuertes Datenbankentwurfstool (DbDesignGenerator), das Benutzer zur Eingabe von Informationen zu den Datenbanken auffordert, die von IBM Business Monitor verwendet werden

(Informationen wie Datenbankplattform und Datenbank, Schema und Benutzernamen). Die Ausgabe des Datenbankentwurfstools ist ein Datenbankentwurfsdokument, das vom Datenbankentwurfstool zum Erstellen der Datenbankskripts verwendet wird.

Gehen Sie wie folgt vor, um die Implementierungsumgebung zu konfigurieren:

1. Klicken Sie in der Administrationskonsole auf **Server > Deployment Environments (Implementierungsumgebungen)**.
2. Klicken Sie zum Starten des Konfigurationsassistenten für Implementierungsumgebungen auf der Seite 'Deployment Environments' auf **New** (Neu).
  - a. Die Option **Create a deployment environment based on a pattern** (Implementierungsumgebung auf Basis eines Musters erstellen) ist ausgewählt.
  - b. Geben Sie einen eindeutigen Namen für die Implementierungsumgebung in das Feld **Deployment environment name** (Name der Implementierungsumgebung) ein.
  - c. Wenn alle Konfigurationsschritte im Assistenten angezeigt werden sollen, wählen Sie **Detailed: Show all steps** (Detailliert: Alle Schritte anzeigen) aus. Bei Auswahl von **Fast path: Show only needed steps** (Schneller Pfad: Nur benötigte Schritte anzeigen) zeigt der Assistent nur die Seiten an, denen keine Standardwerte zugewiesen sind. Wählen Sie **Fast path: Show only needed steps** nur aus, wenn Sie für die Konfiguration der Implementierungsumgebung die vom System vorgegebenen Standardwerte übernehmen wollen. In diesem Abschnitt wird vorausgesetzt, dass Sie die Option **Detailed: Show all steps** ausgewählt haben.
  - d. Klicken Sie auf **Next** (Weiter), um die Seite 'Deployment Environment Features' (Features der Implementierungsumgebung) anzuzeigen.
3. Wählen Sie auf der Seite **Deployment Environment Features** das Feature für die Implementierungsumgebung aus und klicken Sie auf **Next**, um entweder eine Liste der kompatiblen Features oder eine Liste mit Implementierungsumgebungsmustern anzuzeigen. Features stellen die Laufzeitverarbeitungsfunktionalität einer Implementierungsumgebung dar. Die Liste mit verfügbaren Features auf der Seite **Deployment Environment Features** basiert auf dem Deployment Manager-Profil. Wenn Ihr Deployment Manager-Profil um weitere Produkte sowie um IBM Business Monitor (z. B. IBM Business Process Manager) erweitert wurde, dann werden diese Features auch auf der Seite **Deployment Environment Features** (Implementierungsumgebungsfeatures) aufgelistet. Der Standardwert für das Feature der Implementierungsumgebung entspricht der Laufzeitfunktionalität des Deployment Managers.
4. Wählen Sie auf der Seite **Select compatible deployment environment features** (Kompatible Features für Implementierungsumgebung auswählen) bei Bedarf weitere Features aus und klicken Sie auf **Next** (Weiter), um die Liste der Muster anzuzeigen, die denen von Ihnen ausgewählten Features zugeordnet sind. Es kann nur eine Konfiguration der Implementierungsumgebung für eine WBM-Feature geben. Falls bereits eine Konfiguration der Implementierungsumgebung für die WBM-Features vorhanden ist, können Sie nicht fortfahren. Sie können selbst dann nicht fortfahren, wenn die Konfiguration der Implementierungsumgebung noch nicht generiert wurde.
5. Wählen Sie auf der Seite **Select the deployment environment pattern** (Implementierungsumgebungsmuster auswählen) das Muster aus und klicken Sie auf **Next** (Weiter), um die Seite **Select Nodes** (Knoten auswählen) anzuzeigen. Die Liste mit Mustern, die auf der Seite **Deployment Environment Patterns** (Implementierungsumgebungsmuster) angezeigt wird, ist dynamisch. Die Liste

wird durch folgende Umgebungsbedingungen und Konfigurationsentscheidungen aktiviert und ist von diesen abhängig:

- Plattform, auf der Sie die Software installiert haben
- Auswahl, die Sie auf den Seiten **Select the deployment environment feature** und **Select compatible deployment environment features** getroffen haben.

Normalerweise können Sie zwischen dem Ein-Cluster-Muster und dem Vier-Cluster-Muster (Fernes Messaging, Fernunterstützung und Webanwendungen) auswählen. Beschreibungen dieser Muster finden Sie auf der Seite 'Topologie für Hochverfügbarkeit (Network Deployment)' im Planungskapitel.

6. Wählen Sie auf der Seite **Select Nodes** die Knoten aus, die in die Implementierungsumgebung aufgenommen werden sollen, und klicken Sie dann auf **Next** (Weiter), um die Seite **Cluster members** (Cluster-Member) anzuzeigen.

Wählen Sie einen oder mehrere IBM Business Monitor-Knoten für die Implementierungsumgebung aus. Sie können die IBM Business Monitor-Knoten über einen Eintrag für WBM in der Versionsspalte der Liste angeben. Falls ein Knoten über keinen Eintrag für WBM in der Versionsspalte verfügt und Sie ihn für IBM Business Monitor aktivieren möchten, erweitern Sie das Knotenprofil mit IBM Business Monitor und starten Sie den Konfigurationsassistenten für die Implementierungsumgebung erneut.

Alle ausgewählten Knoten müssen IBM Business Monitor-Knoten sein. Wenn Sie zusätzliche Features in Schritt 3 ausgewählt haben, wählen Sie die Knoten aus, die bereits diese zusätzlichen Features unterstützen.

Wählen Sie für Hochverfügbarkeits- und Funktionsübernahmeumgebungen mindestens zwei separate Knoten aus. Wählen Sie für eine bessere Skalierbarkeit mehr als zwei Knoten aus.

Schließen Sie einen Knoten ein, indem Sie das Kontrollkästchen neben dem Knotennamen aktivieren.

7. Ordnen Sie auf der Seite **Cluster** mindestens ein Cluster-Member auf mindestens einem Knoten für jede Funktion der Implementierungsumgebung zu.

Standardmäßig wird auf jedem Knoten für jede Funktion ein einziges Cluster-Member zugewiesen. Sie können die Anzahl ändern, indem Sie die Anzahl in den einzelnen Spalten ändern. In einer Netzimplementierung können Cluster zusammenarbeiten, um in der Umgebung eine bestimmte Funktionalität bereitzustellen. Abhängig von Ihren Anforderungen können Sie jedem Cluster in der Implementierungsumgebung bestimmte Funktionen zuweisen, um Leistung, Funktionsübernahme und Kapazität bereitzustellen.

Der Wert 0 (null) für einen Knoten bedeutet, dass der Knoten abhängig von Features, die Sie ausgewählt haben, nichts zur ausgewählten Funktion beiträgt.

Es muss mindestens ein Cluster-Member für jede Funktion zugeordnet sein. Geben Sie für Hochverfügbarkeits- und Funktionsübernahmeumgebungen mindestens zwei Cluster-Member pro Funktion an. Um eine zusätzliche Skalierbarkeit zu erreichen, geben Sie mehr Cluster-Member für eine Funktion an.

Nach der Zuordnung der Cluster-Member können Sie auf **Weiter** klicken, um die Seiten mit den Clusternamen für jeden Clustertyp der Implementierungsumgebung anzuzeigen. Die angezeigten Unterschritte der Clusterbenennung variieren abhängig vom ausgewählten Implementierungsumgebungsmuster. Wenn Sie Clusternamen oder Cluster-Member-Namen nicht anpassen möchten, verwenden Sie das Navigationsfenster des Assistenten, um direkt zur Seite mit den REST-Services zu gelangen, und fahren mit dem nächsten Schritt fort.

- a. Optional: Passen Sie die Clusternamen und die Cluster-Member-Namen an. Verwenden Sie die Seite für die Clusterbenennung, um die Clusternamen oder die Cluster-Member-Namen für den Clustertyp anzupassen. Sie können ferner die Kurznamen der Cluster und Cluster-Member ändern. Es gibt eine Seite mit Unterschriften für jeden Clustertyp im von Ihnen ausgewählten Muster. Folgende Informationen sind auf den einzelnen Seiten mit den Unterschriften enthalten:

Feld	Description (Beschreibung)	Wert
Cluster	Ein Anzeigefeld für die Angabe der Aufgabe des Clusters.	Der Wert variiert abhängig vom Clustertyp wie folgt: <ul style="list-style-type: none"> <li>• Anwendungsimplementierungsziel</li> <li>• Unterstützende Infrastruktur</li> <li>• Messaging-Infrastruktur</li> <li>• Webanwendungsinfrastruktur</li> </ul> Informationen zu der Aufgabe (Funktion), die von jedem Cluster übernommen wird, finden Sie unter 'Muster für Topologien und Implementierungsumgebungen'.
Clustername	Der vom System generierte Standardwert für den Clusternamen.	Die Standardwerte basieren auf der Namenskonvention für <i>Name der Implementierungsumgebung.Clustertypname</i> , wobei <i>Clustertypname</i> einer der folgenden Werte ist: <ul style="list-style-type: none"> <li>• <b>AppTarget</b> - Für Cluster, die die Aufgabe eines Anwendungsimplementierungsziels übernehmen.</li> <li>• <b>Messaging</b> - Für Cluster, die die Aufgabe einer Messaging-Infrastruktur übernehmen.</li> <li>• <b>Support</b> - Für Cluster, die die Aufgabe einer unterstützenden Infrastruktur übernehmen.</li> <li>• <b>Web</b> - Für Cluster, die die Aufgabe von unterstützenden Webanwendungen übernehmen.</li> </ul>

Feld	Description (Beschreibung)	Wert
Cluster-Member-Name	Der vom System generierte Standardwert für den Cluster-Member-Namen. Server, die Teil eines Clusters sind, werden Cluster-Member genannt.	<p>Akzeptieren Sie den vom System generierten Standardwert oder geben Sie einen Namen Ihrer Wahl an. Der Standardwert für den Cluster-Member-Namen basiert auf folgender Namenskonvention:  <code>clustername.knotenname.knotennummernfolge</code></p> <p>Die Anzahl der Cluster-Member-Namen, die in der Tabelle angezeigt werden, stimmt mit der Anzahl der Cluster-Member überein, die Sie in der Spalte für den Clustertyp in der Knotenzeile auf der Seite für die Cluster angegeben haben.</p>

8. Konfigurieren Sie auf der Seite **System REST Service endpoints** Serviceendpunkte für Representational State Transfer (REST)-Anwendungsprogrammierschnittstellen (APIs).

Wenn Widgets in Business Space verfügbar sein sollen, müssen Sie die REST-Serviceendpunkte für die betreffenden Widgets konfigurieren. Wenn die REST-Anforderungen direkt an den Anwendungsserver weitergeleitet werden sollen, geben Sie den Hostnamen und den Port des Anwendungsservers ein. Wenn die REST-Anforderungen an einen Proxy-Server oder an einen HTTP-Server weitergeleitet werden sollen, der vor einem oder mehreren Anwendungsservern platziert ist, müssen Sie den Hostnamen und Port des Proxy- oder HTTP-Servers eingeben. Im zweiten Fall muss bereits ein Proxy-Server oder ein HTTP-Server definiert sein. Überspringen Sie andernfalls diese Seite und konfigurieren Sie die Endpunkte später.

- a. Konfigurieren Sie einen vollständigen URL-Pfad für alle REST-Services, indem Sie entweder **https://** oder **http://** in der Liste **Protocol** (Protokoll) auswählen.
- b. Geben Sie den Namen des Proxy-Servers oder HTTP-Servers im Feld **Host Name or Virtual Host in a Load-Balanced Environment** (Hostname oder virtueller Host in einer Umgebung mit Lastausgleich) ein.  
 Geben Sie den Host oder den virtuellen Hostnamen und die Portnummer ein, die ein Client benötigt, um mit dem Server oder Cluster zu kommunizieren. In einer Clusterumgebung ist dies in der Regel der Hostname und der Port der Lastausgleichsfunktion. Wenn Sie die Felder für den Host und den Port leer lassen, werden standardmäßig die Werte eines einzelnen Cluster-Member-Hosts und dessen HTTP-Port angenommen. Bei einer Umgebung mit Lastausgleich, müssen Sie die Standardwerte später in den virtuellen Hostnamen und Port für Ihre Lastausgleichsfunktion ändern. Stellen Sie sicher, dass Sie einen vollständig qualifizierter Hostnamen angeben.
- c. Geben Sie im Feld **Port** den Port ein, den ein Client zur Kommunikation mit dem Server oder Cluster benötigt.
- d. Wenn Sie die Beschreibung des REST-Serviceendpunkts ändern möchten, überschreiben Sie in der Tabelle mit den REST-Services den Eintrag im Beschreibungsfeld. Die übrigen Felder sind schreibgeschützt.
- e. Klicken Sie auf **Next** (Weiter), um zur Seite **Import the database configuration** (Datenbankkonfiguration importieren) zu gehen.

9. Optional: Klicken Sie auf der Seite **Import the database configuration** (Datenbankkonfiguration importieren) auf **Browse** (Durchsuchen), um das Datenbankentwurfsskizzen-Dokument auszuwählen, oder geben Sie den Pfad des Datenbankentwurfsskizzen-Dokuments ein und klicken Sie dann auf **Next** (Weiter), um zur Seite **Data sources** (Datenquellen) zu gelangen. Wenn Sie ein Entwurfsskizzen-Dokument importieren, werden die Informationen des Entwurfsskizzen-Dokuments auf der Datenbankseite des Assistenten wiedergegeben. Das Entwurfsskizzen-Dokument kann auf einem Datenbankentwurf basieren, den Sie mit dem Datenbankentwurfstool erstellt haben, oder es kann das bereitgestellte Entwurfsskizzen-Dokument auf Basis des ausgewählten Musters und Features sein.
10. Konfigurieren Sie auf der Seite **Database** (Datenbank) die Datenbankparameter für Datenquellen der Implementierungsumgebung und klicken Sie dann auf **Next** (Weiter), um zur Seite **Security** (Sicherheit) zu gelangen.

Definieren Sie auf dieser Seite die Datenbankinformationen für die Komponenten, die in dieser Implementierungsumgebung enthalten sind. Wo dies möglich ist, stellt der Assistent Standardinformationen für die Parameter bereit. Ändern Sie diese Werte so, dass sie mit den Werten übereinstimmen, die Sie bei der Planung der Umgebung festgelegt haben. Bei einem Wechsel des Providers können Sie auf die Schaltfläche **Edit Provider** (Provider bearbeiten) klicken, um den ausgewählten Provider zu bearbeiten.

**Anmerkung:** Wenn Sie ein Datenbankentwurfsskizzen-Dokument importiert haben, geben die Informationen auf der Seite **Database** die Datenquellenkonfiguration so wieder, wie sie im importierten Datenbankentwurfsskizzen-Dokument enthalten ist. Wenn Sie Änderungen an der Datenquellenkonfiguration vornehmen, nachdem ein Datenbankentwurfsskizzen-Dokument importiert wurde, so sind Ihre Änderungen möglicherweise nicht mit der vom Datenbankentwurfstool und den ursprünglichen Werten generierten DDL kompatibel.

Ob dieser Schritt bei einer schnellen Konfiguration der Implementierungsumgebung angezeigt wird, ist von Bedingungen abhängig. Der Schritt wird bei einer schnellen Konfiguration der Implementierungsumgebung angezeigt, wenn mehr als eine Datenbank definiert wurde.

Der Schritt wird immer angezeigt, wenn Sie einen DB2 for z/OS - oder Oracle -Datenbankprovider verwenden.

Das Feature IBM Business Monitor stellt die folgenden Einträge zur Verfügung:

Komponente	Datenquelle
Business Monitor Messaging-Steuerkomponentendatenquelle	Datenquelle für die Messaging-Steuerkomponente von IBM Business Monitor



Komponente	Datenquelle
Cognos-Content-Store	<p>Datenquelle für den IBM Cognos Business Intelligence-Content-Store. (Die Anzeige erfolgt nur, wenn IBM Cognos BI zwar installiert, aber noch nicht konfiguriert wurde.)</p> <p>Die Content-Store-Datenquelle wird in der IBM Cognos BI-Konfiguration und nicht als WebSphere-Datenquelle erstellt. Behalten Sie die Auswahl der Option <b>Tabellen erstellen</b> bei; andernfalls wird diese Datenquelle als verzögerte Konfiguration markiert. IBM Cognos BI erstellt die Tabellen beim ersten Start.</p> <p>Ein WebSphere-Authentifizierungsalias (Cognos_JDBC_Alias) wird auf der Basis des Benutzernamens und Kennworts erstellt, die für diese Datenquelle angegeben wurden. Dieser Authentifizierungsalias wird nicht direkt von IBM Cognos BI verwendet, sondern er ermöglicht die Verwaltung aller Benutzernamen und Kennwörter für die Datenbank mit demselben Prozess. Beim Serverstart sendet IBM Business Monitor die aktuellen Werte für den Benutzernamen und das Kennwort an die IBM Cognos BI-Konfiguration.</p> <p>Für DB2 unter z/OS müssen Sie die COGNOSCS-Datenbank manuell installieren.</p>
Business Space	<p>Datenquelle für die Komponente Business Space. Wenn Sie die Option <b>Tabellen erstellen</b> auswählen, muss der von Business Space verwendete Schemaname bereits in der Datenbank vorhanden sein.</p> <p><b>Wichtig:</b> Nur für Oracle: Sie müssen <code>application_server-stammverzeichnis/dbscripts/BusinessSpace/Oracle/createSchema_BusinessSpace.sql</code> ausführen, um den Schemabeanutzer zu erstellen und die erforderlichen Berechtigungen zu erteilen.</p>

Wenn Sie andere Produktfeatures für diese Topologie ausgewählt haben, können hier auch andere featurespezifische Einträge angezeigt werden.

Die Standardschemanamen, die auf dieser Seite angezeigt werden, verstoßen möglicherweise gegen Ihre Namenskonvention für Sites oder kollidieren mit vorhandenen Schemas. Deshalb werden Sie den Schemanamen ändern müssen.

**Anmerkung:** Bei DB2 for z/OS-Datenbanken wird der Schemaname, der in der Anzeige konfiguriert wurde, für die SQL-Berechtigungs-ID (SQLID) von DB2 z/OS verwendet. Wenn der Wert für die SQL-Berechtigungs-ID von DB2 z/OS in Ihrer Umgebung anders lauten muss, können Sie die erstellten Datenquellen manuell aktualisieren, nachdem der Implementierungsumgebungsassistent abgeschlossen ist, und die angepasste Eigenschaft 'currentSQLID' in den korrekten Wert ändern.

Sie können alle Schlüsselparameter bearbeiten, wie z. B. den Datenbanknamen, die Angabe, ob Tabellen erstellt werden sollen, den Laufzeitbenutzernamen für die Datenquelle oder den Benutzernamen und das Kennwort für die Datenquelle zur Herstellung der Verbindung mit der Datenbank.

**Anmerkung:** Für DB2 for z/OS-Datenbanken ist der Datenbankname der Datenbanksystemname. Für andere Versionen von DB2 ist der Datenbankname der Name der Monitor-Datenbank. Für Oracle-Datenbanken ist der Datenbankname die Oracle System-ID.

Sie können auswählen, welche Datenbank für die angegebene Komponente verwendet werden soll.

Die Option **Tabellen erstellen** ist nicht verfügbar, wenn Sie einen DB2 for z/OS- oder einen Oracle-Datenbankprovider verwenden.

Für Oracle ist das Feld **Schema** inaktiviert und leer und das Feld **User name** (Benutzername) ist nicht bereits mit dem allgemeinen Datenbankbenutzernamen gefüllt. Sie müssen einen Benutzernamen und ein Kennwort für jede Datenquelle eingeben.

**Anmerkung:** Es findet keine Überprüfung statt, um sicherzustellen, dass Benutzernamen eindeutig sind. Achten Sie deshalb darauf, keinen doppelten Benutzernamen zu erstellen, denn dies führt zu Tabellenkonflikten.

11. Geben Sie auf der Seite **Sicherheit** die Benutzer-IDs und Kennwörter ein, die für die Konfiguration der Komponenten von IBM Business Monitor erforderlich sind. Das Feature IBM Business Monitor stellt die folgenden Einträge zur Verfügung:

Komponente	ID und Kennwort
Authentifizierungsalias für die JMS-Ressourcen des CEI-Ereignisservice	Geben Sie die Benutzer-ID und das Kennwort zum Sichern des standardmäßigen CEI-Serviceintegrationsbus an.
Cognos-Zugriffsauthentifizierung für Verwaltungszwecke	Geben Sie eine Benutzer-ID und ein Kennwort mit Administratorberechtigungen für den IBM Cognos BI-Service an. (Die Anzeige erfolgt nur, wenn IBM Cognos BI zwar installiert, aber noch nicht konfiguriert wurde.)

Wenn Sie andere Produktfeatures für diese Topologie ausgewählt haben, können hier auch andere featurespezifische Einträge angezeigt werden.

12. Optional: Wenn die Seite 'Business Process Choreographer' angezeigt wird, legen Sie Parameter für die Business Process Choreographer-Konfiguration fest und klicken anschließend auf **Next** (Weiter), um die Seite **Web application context roots** (Stammkontexte für Webanwendung) anzuzeigen. Auf dieser Seite geben Sie Werte an für:

- Sicherheitsrollen
- Authentifizierungsaliasnamen

13. Optional: Wenn die Seite **Web application context roots** (Stammkontexte für Webanwendung) angezeigt wird, legen Sie das Kontextstammverzeichnis für komponentenbasierte Webanwendungen in Ihrer Implementierungsumgebung fest oder akzeptieren die vom System bereitgestellten Standardwerte für die Kontextstammverzeichnisse. Klicken Sie dann auf **Next** (Weiter), um die Seite **Summary** (Zusammenfassung) anzuzeigen.

Die Tabelle enthält folgende Steuerinformationen:

**Web Application (Webanwendung)**

Der Name der Webanwendung.

Einige der Komponenten, die Teil der von Ihnen erstellten Implementierungsumgebung sind, enthalten Webanwendungen. Die Spalte **Web application** kann folgende Komponenten enthalten:

- Business Process Choreographer Explorer

- Business Space
- Business Process Rules Manager

#### **Context Root (Kontextstammverzeichnis)**

Der aktuelle Wert des Kontextstammverzeichnisses für die Komponente.

Dabei handelt es sich standardmäßig um das Standardkontextstammverzeichnis für die Webanwendung. Sie können die Kontextstammverzeichnisse ändern, indem Sie den Wert im Feld **Context Root** überschreiben.

**Anmerkung:** Das Business Space-Kontextstammverzeichnis wird nur gelesen und kann nicht bearbeitet werden.

14. Prüfen Sie, ob die Informationen auf der Seite **Summary** korrekt sind, und klicken Sie auf **Finish and Generate Environment** (Umgebung fertig stellen und generieren), um die Konfiguration der Implementierungsumgebung zu speichern und abzuschließen. Klicken Sie auf **Finish** (Fertig stellen), wenn Sie die Konfiguration beenden möchten, ohne sie abzuschließen.

Beim Klicken auf **Finish** wird die Implementierungsumgebung gespeichert - aber sie wird nicht generiert.

Wenn Sie auf **Cancel** (Abbrechen) klicken, wird die Implementierungskonfiguration abgebrochen und nicht gespeichert.

15. Wenn Sie auf **Finish and Generate Environment** (Umgebung fertig stellen und generieren) geklickt haben, um die Implementierungsumgebung zu generieren, stoppen Sie alle Cluster, Knoten und den Deployment Manager und starten Sie diese Komponenten erneut.

Wenn Sie ausgewählt haben, dass Sie die Umgebung nicht am Ende der Konfiguration der Implementierungsumgebung mit dem Assistenten generieren möchten (indem Sie auf **Finish (Fertig stellen)** und nicht auf **Finish and Generate Environment (Umgebung fertig stellen und generieren)** klicken), können Sie die Implementierungsumgebungskonfiguration unter **Server > Deployment Environments (Implementierungsumgebungen) > name der Implementierungsumgebung** anzeigen. Von dieser Position aus können Sie auf **Generieren** klicken, um die Umgebung zu generieren. Nach Abschluss der Konfiguration können Sie die Konfigurationsdateien überprüfen, um die Änderungen anzuzeigen.

Speichern Sie die Änderungen in der Masterkonfiguration oder verwerfen Sie sie. Wenn Sie auf eine Implementierungsumgebung in der Liste klicken und noch Konfigurationsschritte auszuführen sind, sehen Sie eine Liste mit den aufgeschobenen Konfigurationsschritten. Nach der Generierung einer Implementierungsumgebung sollten alle Cluster, Knoten und der Deployment Manager gestoppt und erneut gestartet werden.

**Wichtig:** Das Cluster, das den IBM Cognos BI-Dienst ausführt, erfordert den Einzelstart jedes einzelnen Cluster-Members. Sie müssen die vollständige Initialisierung des IBM Cognos BI-Dienstes abwarten, bevor Sie das nächste Cluster-Member starten.

## **Auf Gestaltungsdokumenten basierende Implementierungsumgebungsdefinitionen importieren**

Sie können eine auf einem Gestaltungsdokument basierende Implementierungsumgebungsdefinition von einem anderen Deployment Manager importieren, um diese als Basis für die Konfiguration einer neuen Implementierungsumgebung zu verwenden.

- Sie müssen über eine Kopie eines exportierten Implementierungsumgebungs-gestaltungsdokuments eines anderen Deployment Managers verfügen.
- Sie müssen auf das Gestaltungsdokument der Implementierungsumgebung (eine XML-Datei) von dem Deployment Manager zugreifen können, in den Sie das Gestaltungsdokument der Implementierungsumgebung importieren.
- Der Deployment Manager, der die Implementierungsumgebungsdefinition im-portiert, muss zumindest die Funktionen unterstützen, die im Gestaltungsdoku-ment der Implementierungsumgebung definiert sind. Sie können beispielsweise eine auf einem WebSphere Enterprise Service Bus-Deployment Manager erstellte Implementierungsumgebungsgestaltung in einen Process Server-Deployment Manager importieren, aber nicht umgekehrt.

**Anmerkung:** Wenn Sicherheit und rollenbasierte Berechtigung aktiviert sind, müs-sen Sie sich als Administrator an der Administrationskonsole anmelden, um diese Task ausführen zu können.

**Wichtig:** Der gleichzeitige Import mehrerer Gestaltungsdokumente der Implemen-tierungsumgebung aus einer komprimierten Datei ist nicht möglich. Die Gestal-tungsdokumente müssen aus der komprimierten Datei extrahiert und anschließend nacheinander in die XML-Dateien importiert werden.

Stellen Sie vor dem Starten des Konfigurationsprozesses sicher, dass Sie Änderun-gen am Knoten automatisch synchronisieren (klicken Sie in der Administrations-konsole auf **Systemverwaltung > Konsoleinstellungen** und wählen Sie **Änderun-gen mit Knoten synchronisieren**) aus. Andernfalls müssen Sie die Änderungen nach jedem Hauptschritt manuell synchronisieren.

Der Import eines bereits vorhandenen Implementierungsumgebungsdesigns zur Er-stellung eines neuen kann die zur Konfiguration einer Implementierungsumgebung erforderliche Zeit verringern. Wenn eine bereits vorhandene Umgebung der Umge-bung ähnelt, die Sie erstellen möchten, exportieren Sie diese und importieren Sie sie anschließend in den Deployment Manager, den Sie konfigurieren.

1. Klicken Sie in der Administrationskonsole auf **Server > Deployment Environ-ments (Implementierungsumgebungen)**.
2. Klicken Sie auf der Seite **Deployment Environments (Implementierungsum-gebungen)** auf **Import**, um den Assistenten **Deployment Environment Confi-guration** (Implementierungsumgebungskonfiguration) zu starten.

Beim Start des Assistenten ist die Option **Create a deployment environment based on an imported design** (Implementierungsumgebung auf der Basis ei-nes importierten Designs erstellen) bereits ausgewählt.

3. Klicken Sie auf **Durchsuchen** und wählen Sie das zu importierende Gestal-tungsdokument der Implementierungsumgebung (XML-Datei) aus oder geben Sie den vollständigen Pfad des Dokuments ein.
4. Klicken Sie auf **Weiter**, um die Konfiguration zu laden und den Assistenten **Import deployment environment** (Implementierungsumgebungsassistent im-portieren) zu starten.

Der Assistent zeigt die Seite **Select Nodes** (Knoten auswählen) an, es sei denn alle Knotennamen stimmen mit derzeit eingebundenen Knoten überein. Wenn alle Knoten übereinstimmen, zeigt der Assistent die Seite **Database** (Daten-bank) an.

**Wichtig:** Durch Anklicken der Option 'Configure' (Konfigurieren) in einer be-liebigen Anzeige des Assistenten wird die Implementierungsumgebung mit den aktuellen Werten konfiguriert.

5. Optional: Wählen Sie in der Liste der möglichen Knoten auf der Seite **Select Nodes** (Knoten auswählen) die Knoten aus, die in die Implementierungsumgebung aufgenommen werden sollen und klicken Sie auf **Weiter**.

Schließen Sie einen Knoten ein, indem Sie das Kontrollkästchen neben dem Knotennamen aktivieren.

**Wichtig:** Die Option **Weiter** ist nicht verfügbar, wenn die ausgewählten Knoten den Einschränkungen des importierten Implementierungsumgebungsdesigns nicht entsprechen. Wenn beispielsweise eine Voraussetzung der Implementierungsumgebung ist, dass ein Knoten mit der Bezeichnung „Mandatory\_Node“ (Obligatorischer Knoten) sowie 3 andere Knoten mit beliebigen Namen enthalten sein müssen, können Sie erst fortfahren, wenn Sie „Mandatory\_Node“ (Obligatorischer Knoten) und 3 weitere Knoten ausgewählt haben.

6. Ordnen Sie auf der Seite **Cluster** mindestens ein Cluster-Member auf mindestens einem Knoten für jede Funktion der Implementierungsumgebung zu.

Standardmäßig wird auf jedem Knoten für jede Funktion ein einziges Cluster-Member zugewiesen. Sie können die Anzahl ändern, indem Sie die Anzahl in den einzelnen Spalten ändern. In einer Netzimplementierung können Cluster zusammenarbeiten, um in der Umgebung eine bestimmte Funktionalität bereitzustellen. Abhängig von Ihren Anforderungen können Sie jedem Cluster in der Implementierungsumgebung bestimmte Funktionen zuweisen, um Leistung, Funktionsübernahme und Kapazität bereitzustellen.

Der Wert 0 (null) für einen Knoten bedeutet, dass der Knoten abhängig von Features, die Sie ausgewählt haben, nichts zur ausgewählten Funktion beiträgt.

Es muss mindestens ein Cluster-Member für jede Funktion zugeordnet sein. Geben Sie für Hochverfügbarkeits- und Funktionsübernahmeumgebungen mindestens zwei Cluster-Member pro Funktion an. Um eine zusätzliche Skalierbarkeit zu erreichen, geben Sie mehr Cluster-Member für eine Funktion an.

Nach der Zuordnung der Cluster-Member können Sie auf **Weiter** klicken, um die Seiten mit den Clusternamen für jeden Clustertyp der Implementierungsumgebung anzuzeigen. Die angezeigten Unterschritte der Clusterbenennung variieren abhängig vom ausgewählten Implementierungsumgebungsdesign. Wenn Sie Clusternamen oder Cluster-Member-Namen nicht anpassen möchten, verwenden Sie das Navigationsfenster des Assistenten, um direkt zur Seite mit den REST-Services zu gelangen, und fahren mit dem nächsten Schritt fort.

- a. Optional: Passen Sie die Clusternamen und die Cluster-Member-Namen an. Verwenden Sie die Seite für die Clusterbenennung, um die Clusternamen oder die Cluster-Member-Namen für den Clustertyp anzupassen. Sie können ferner die Kurznamen der Cluster und Cluster-Member ändern. Es gibt eine Seite mit Unterschritten für jeden Clustertyp im von Ihnen ausgewählten Muster. Folgende Informationen sind auf den einzelnen Seiten mit den Unterschritten enthalten:

Feld	Description (Beschreibung)	Wert
Cluster	Ein Anzeigefeld für die Angabe der Aufgabe des Clusters.	<p>Der Wert variiert abhängig vom Clustertyp wie folgt:</p> <ul style="list-style-type: none"> <li>• Anwendungsimplementierungsziel</li> <li>• Unterstützende Infrastruktur</li> <li>• Messaging-Infrastruktur</li> <li>• Webanwendungsinfrastruktur</li> </ul> <p>Informationen zu der Aufgabe (Funktion), die von jedem Cluster übernommen wird, finden Sie unter 'Muster für Topologien und Implementierungsumgebungen'.</p>
Clustername	Der vom System generierte Standardwert für den Clusternamen.	<p>Die Standardwerte basieren auf der Namenskonvention für <i>Name der Implementierungsumgebung.Clustertypname</i>, wobei <i>Clustertypname</i> einer der folgenden Werte ist:</p> <ul style="list-style-type: none"> <li>• <b>AppTarget</b> - Für Cluster, die die Aufgabe eines Anwendungsimplementierungsziels übernehmen.</li> <li>• <b>Messaging</b> - Für Cluster, die die Aufgabe einer Messaging-Infrastruktur übernehmen.</li> <li>• <b>Support</b> - Für Cluster, die die Aufgabe einer unterstützenden Infrastruktur übernehmen.</li> <li>• <b>Web</b> - Für Cluster, die die Aufgabe von unterstützenden Webanwendungen übernehmen.</li> </ul>
Cluster-Member-Name	Der vom System generierte Standardwert für den Cluster-Member-Namen. Server, die Teil eines Clusters sind, werden Cluster-Member genannt.	<p>Akzeptieren Sie den vom System generierten Standardwert oder geben Sie einen Namen Ihrer Wahl an. Der Standardwert für den Cluster-Member-Namen basiert auf folgender Namenskonvention:  <i>clustername.knotenname.knotennummernfolge</i>.  Die Anzahl der Cluster-Member-Namen, die in der Tabelle angezeigt werden, stimmt mit der Anzahl der Cluster-Member überein, die Sie in der Spalte für den Clustertyp in der Knotenzeile auf der Seite für die Cluster angegeben haben.</p>



7. Konfigurieren Sie auf der Seite **System REST Service endpoints** Serviceendpunkte für Representational State Transfer (REST)-Anwendungsprogrammierschnittstellen (APIs).

Wenn Widgets in Business Space verfügbar sein sollen, müssen Sie die REST-Serviceendpunkte für die betreffenden Widgets konfigurieren. Wenn die REST-Anforderungen direkt an den Anwendungsserver weitergeleitet werden sollen, geben Sie den Hostnamen und den Port des Anwendungsservers ein. Wenn die REST-Anforderungen an einen Proxy-Server oder an einen HTTP-Server weitergeleitet werden sollen, der vor einem oder mehreren Anwendungsservern platziert ist, müssen Sie den Hostnamen und Port des Proxy- oder HTTP-Servers eingeben. Im zweiten Fall muss bereits ein Proxy-Server oder ein HTTP-Server definiert sein. Überspringen Sie andernfalls diese Seite und konfigurieren Sie die Endpunkte später.

- a. Konfigurieren Sie einen vollständigen URL-Pfad für alle REST-Services, indem Sie entweder **https://** oder **http://** in der Liste **Protocol** (Protokoll) auswählen.
  - b. Geben Sie den Namen des Proxy-Servers oder HTTP-Servers im Feld **Host Name or Virtual Host in a Load-Balanced Environment** (Hostname oder virtueller Host in einer Umgebung mit Lastausgleich) ein.  
Geben Sie den Host oder den virtuellen Hostnamen und die Portnummer ein, die ein Client benötigt, um mit dem Server oder Cluster zu kommunizieren. In einer Clusterumgebung ist dies in der Regel der Hostname und der Port der Lastausgleichsfunktion. Wenn Sie die Felder für den Host und den Port leer lassen, werden standardmäßig die Werte eines einzelnen Cluster-Member-Hosts und dessen HTTP-Port angenommen. Bei einer Umgebung mit Lastausgleich, müssen Sie die Standardwerte später in den virtuellen Hostnamen und Port für Ihre Lastausgleichsfunktion ändern. Stellen Sie sicher, dass Sie einen vollständig qualifizierter Hostnamen angeben.
  - c. Geben Sie im Feld **Port** den Port ein, den ein Client zur Kommunikation mit dem Server oder Cluster benötigt.
  - d. Wenn Sie die Beschreibung des REST-Serviceendpunkts ändern möchten, überschreiben Sie in der Tabelle mit den REST-Services den Eintrag im Beschreibungsfeld. Die übrigen Felder sind schreibgeschützt.
  - e. Klicken Sie auf **Next** (Weiter), um zur Seite **Import the database configuration** (Datenbankkonfiguration importieren) zu gehen.
8. Optional: Klicken Sie auf der Seite **Import the database configuration** (Datenbankkonfiguration importieren) auf **Browse** (Durchsuchen), um das Datenbankentwurfsdokument auszuwählen, oder geben Sie den Pfad des Datenbankentwurfsdokuments ein und klicken Sie dann auf **Next** (Weiter), um zur Seite **Data sources** (Datenquellen) zu gelangen. Wenn Sie ein Entwurfsdokument importieren, werden die Informationen des Entwurfsdokuments auf der Datenbankseite des Assistenten wiedergegeben. Das Entwurfsdokument kann auf einem Datenbankentwurf basieren, den Sie mit dem Datenbankentwurfstool erstellt haben, oder es kann das bereitgestellte Entwurfsdokument auf Basis des ausgewählten Musters und Features sein.
  9. Konfigurieren Sie auf der Seite **Database** (Datenbank) die Datenbankparameter für Datenquellen der Implementierungsumgebung und klicken Sie dann auf **Next** (Weiter), um zur Seite **Security** (Sicherheit) zu gelangen.

Definieren Sie auf dieser Seite die Datenbankinformationen für die Komponenten, die in dieser Implementierungsumgebung enthalten sind. Wo dies möglich ist, stellt der Assistent Standardinformationen für die Parameter bereit. Ändern Sie diese Werte so, dass sie mit den Werten übereinstimmen, die Sie bei der Planung der Umgebung festgelegt haben. Bei einem Wechsel des



Providers können Sie auf die Schaltfläche **Edit Provider** (Provider bearbeiten) klicken, um den ausgewählten Provider zu bearbeiten.

**Anmerkung:** Wenn Sie ein Datenbankentwurfsdokument importiert haben, geben die Informationen auf der Seite **Database** die Datenquellenkonfiguration so wieder, wie sie im importierten Datenbankentwurfsdokument enthalten ist. Wenn Sie Änderungen an der Datenquellenkonfiguration vornehmen, nachdem ein Datenbankentwurfsdokument importiert wurde, so sind Ihre Änderungen möglicherweise nicht mit der vom Datenbankentwurfstool und den ursprünglichen Werten generierten DDL kompatibel.

Ob dieser Schritt bei einer schnellen Konfiguration der Implementierungsumgebung angezeigt wird, ist von Bedingungen abhängig. Der Schritt wird bei einer schnellen Konfiguration der Implementierungsumgebung angezeigt, wenn mehr als eine Datenbank definiert wurde.

Der Schritt wird immer angezeigt, wenn Sie einen DB2 for z/OS - oder Oracle -Datenbankprovider verwenden.

Das Feature IBM Business Monitor stellt die folgenden Einträge zur Verfügung:

Komponente	Datenquelle
Business Monitor Messaging-Steuerkomponentendatenquelle	Datenquelle für die Messaging-Steuerkomponente von IBM Business Monitor
Cognos-Content-Store	<p>Datenquelle für den IBM Cognos Business Intelligence-Content-Store. (Die Anzeige erfolgt nur, wenn IBM Cognos BI zwar installiert, aber noch nicht konfiguriert wurde.)</p> <p>Die Content-Store-Datenquelle wird in der IBM Cognos BI-Konfiguration und nicht als WebSphere-Datenquelle erstellt. Behalten Sie die Auswahl der Option <b>Tabellen erstellen</b> bei; andernfalls wird diese Datenquelle als verzögerte Konfiguration markiert. IBM Cognos BI erstellt die Tabellen beim ersten Start.</p> <p>Ein WebSphere-Authentifizierungsalias (Cognos_JDBC_Alias) wird auf der Basis des Benutzernamens und Kennworts erstellt, die für diese Datenquelle angegeben wurden. Dieser Authentifizierungsalias wird nicht direkt von IBM Cognos BI verwendet, sondern er ermöglicht die Verwaltung aller Benutzernamen und Kennwörter für die Datenbank mit demselben Prozess. Beim Serverstart sendet IBM Business Monitor die aktuellen Werte für den Benutzernamen und das Kennwort an die IBM Cognos BI-Konfiguration.</p> <p>Für DB2 unter z/OS müssen Sie die COGNOSCS-Datenbank manuell installieren.</p>
Business Space	<p>Datenquelle für die Komponente Business Space. Wenn Sie die Option <b>Tabellen erstellen</b> auswählen, muss der von Business Space verwendete Schemaname bereits in der Datenbank vorhanden sein.</p> <p><b>Wichtig:</b> Nur für Oracle: Sie müssen <code>application_server-stammverzeichnis/dbscripts/BusinessSpace/Oracle/createSchema_BusinessSpace.sql</code> ausführen, um den Schemabeneutzer zu erstellen und die erforderlichen Berechtigungen zu erteilen.</p>

Wenn Sie andere Produktfeatures für diese Topologie ausgewählt haben, können hier auch andere featurespezifische Einträge angezeigt werden.

Die Standardschemanamen, die auf dieser Seite angezeigt werden, verstoßen möglicherweise gegen Ihre Namenskonvention für Sites oder kollidieren mit vorhandenen Schemas. Deshalb werden Sie den Schemanamen ändern müssen.

**Anmerkung:** Bei DB2 for z/OS-Datenbanken wird der Schemaname, der in der Anzeige konfiguriert wurde, für die SQL-Berechtigungs-ID (SQLID) von DB2 z/OS verwendet. Wenn der Wert für die SQL-Berechtigungs-ID von DB2 z/OS in Ihrer Umgebung anders lauten muss, können Sie die erstellten Datenquellen manuell aktualisieren, nachdem der Implementierungsumgebungsassistent abgeschlossen ist, und die angepasste Eigenschaft 'currentSQLID' in den korrekten Wert ändern.

Sie können alle Schlüsselparameter bearbeiten, wie z. B. den Datenbanknamen, die Angabe, ob Tabellen erstellt werden sollen, den Laufzeitbenutzernamen für die Datenquelle oder den Benutzernamen und das Kennwort für die Datenquelle zur Herstellung der Verbindung mit der Datenbank.

**Anmerkung:** Für DB2 for z/OS-Datenbanken ist der Datenbankname der Datenbanksystemname. Für andere Versionen von DB2 ist der Datenbankname der Name der Monitor-Datenbank. Für Oracle-Datenbanken ist der Datenbankname die Oracle System-ID.

Sie können auswählen, welche Datenbank für die angegebene Komponente verwendet werden soll.

Die Option **Tabellen erstellen** ist nicht verfügbar, wenn Sie einen DB2 for z/OS- oder einen Oracle-Datenbankprovider verwenden.

Für Oracle ist das Feld **Schema** inaktiviert und leer und das Feld **User name** (Benutzername) ist nicht bereits mit dem allgemeinen Datenbankbenutzernamen gefüllt. Sie müssen einen Benutzernamen und ein Kennwort für jede Datenquelle eingeben.

**Anmerkung:** Es findet keine Überprüfung statt, um sicherzustellen, dass Benutzernamen eindeutig sind. Achten Sie deshalb darauf, keinen doppelten Benutzernamen zu erstellen, denn dies führt zu Tabellenkonflikten.

10. Geben Sie auf der Seite **Sicherheit** die Benutzer-IDs und Kennwörter ein, die für die Konfiguration der Komponenten von IBM Business Monitor erforderlich sind. Das Feature IBM Business Monitor stellt die folgenden Einträge zur Verfügung:

Komponente	ID und Kennwort
Authentifizierungsalias für die JMS-Ressourcen des CEI-Ereignisservice	Geben Sie die Benutzer-ID und das Kennwort zum Sichern des standardmäßigen CEI-Serviceintegrationsbus an.
Cognos-Zugriffsauthentifizierung für Verwaltungszwecke	Geben Sie eine Benutzer-ID und ein Kennwort mit Administratorberechtigungen für den IBM Cognos BI-Service an. (Die Anzeige erfolgt nur, wenn IBM Cognos BI zwar installiert, aber noch nicht konfiguriert wurde.)

Wenn Sie andere Produktfeatures für diese Topologie ausgewählt haben, können hier auch andere featurespezifische Einträge angezeigt werden.

11. Optional: Wenn die Seite 'Business Process Choreographer' angezeigt wird, legen Sie Parameter für die Business Process Choreographer-Konfiguration fest

und klicken anschließend auf **Next** (Weiter), um die Seite **Web application context roots** (Stammkontexte für Webanwendung) anzuzeigen. Auf dieser Seite geben Sie Werte an für:

- Sicherheitsrollen
  - Authentifizierungsaliasnamen
12. Optional: Wenn die Seite **Web application context roots** (Stammkontexte für Webanwendung) angezeigt wird, legen Sie das Kontextstammverzeichnis für komponentenbasierte Webanwendungen in Ihrer Implementierungsumgebung fest oder akzeptieren die vom System bereitgestellten Standardwerte für die Kontextstammverzeichnisse. Klicken Sie dann auf **Next** (Weiter), um die Seite **Summary** (Zusammenfassung) anzuzeigen.

Die Tabelle enthält folgende Steuerinformationen:

#### **Web Application (Webanwendung)**

Der Name der Webanwendung.

Einige der Komponenten, die Teil der von Ihnen erstellten Implementierungsumgebung sind, enthalten Webanwendungen. Die Spalte **Web application** kann folgende Komponenten enthalten:

- Business Process Choreographer Explorer
- Business Space
- Business Process Rules Manager

#### **Context Root (Kontextstammverzeichnis)**

Der aktuelle Wert des Kontextstammverzeichnisses für die Komponente.

Dabei handelt es sich standardmäßig um das Standardkontextstammverzeichnis für die Webanwendung. Sie können die Kontextstammverzeichnisse ändern, indem Sie den Wert im Feld **Context Root** überschreiben.

**Anmerkung:** Das Business Space-Kontextstammverzeichnis wird nur gelesen und kann nicht bearbeitet werden.

13. Prüfen Sie, ob die Informationen auf der Seite **Summary** korrekt sind, und klicken Sie auf **Finish and Generate Environment** (Umgebung fertig stellen und generieren), um die Konfiguration der Implementierungsumgebung zu speichern und abzuschließen. Klicken Sie auf **Finish** (Fertig stellen), wenn Sie die Konfiguration beenden möchten, ohne sie abzuschließen.

Beim Klicken auf **Finish** wird die Implementierungsumgebung gespeichert - aber sie wird nicht generiert.

Wenn Sie auf **Cancel** (Abbrechen) klicken, wird die Implementierungskonfiguration abgebrochen und nicht gespeichert.

14. Wenn Sie auf **Finish and Generate Environment** (Umgebung fertig stellen und generieren) geklickt haben, um die Implementierungsumgebung zu generieren, stoppen Sie alle Cluster, Knoten und den Deployment Manager und starten Sie diese Komponenten erneut.

Wenn Sie ausgewählt haben, dass Sie die Umgebung nicht am Ende der Konfiguration der Implementierungsumgebung mit dem Assistenten generieren möchten (indem Sie auf **Finish (Fertig stellen)** und nicht auf **Finish and Generate Environment (Umgebung fertig stellen und generieren)** klicken), können Sie die Implementierungsumgebungskonfiguration unter **Server > Deployment Environments (Implementierungsumgebungen) > name der Implementierungsumgebung** anzeigen. Von dieser Position aus können Sie auf **Generieren** klicken, um die Umgebung zu generieren. Nach Abschluss der Konfiguration können Sie die Konfigurationsdateien überprüfen, um die Änderungen anzuzeigen.

Speichern Sie die Änderungen in der Masterkonfiguration oder verwerfen Sie sie. Wenn Sie auf eine Implementierungsumgebung in der Liste klicken und noch Konfigurationsschritte auszuführen sind, sehen Sie eine Liste mit den aufgeschobenen Konfigurationsschritten. Nach der Generierung einer Implementierungsumgebung sollten alle Cluster, Knoten und der Deployment Manager gestoppt und erneut gestartet werden.

**Wichtig:** Das Cluster, das den IBM Cognos BI-Dienst ausführt, erfordert den Einzelstart jedes einzelnen Cluster-Members. Sie müssen die vollständige Initialisierung des IBM Cognos BI-Dienstes abwarten, bevor Sie das nächste Cluster-Member starten.

## IBM Business Monitor-Implementierungsumgebung einer IBM Business Process Manager-Serverimplementierungsumgebung hinzufügen

Wenn eine IBM Business Monitor-Implementierungsumgebung mit dem Konfigurationsassistenten für Implementierungsumgebungen einer vorhandenen IBM Business Process Manager-Implementierungsumgebung hinzugefügt wird, sind einige zusätzliche Schritte auszuführen.

Sie müssen entweder die IBM BPM-Widgets in IBM Business Monitor Business Space installieren und registrieren (die einfachste und daher bevorzugte Methode) oder die IBM Business Monitor-Widgets in IBM BPM Business Space installieren und registrieren.

Erstellen Sie die IBM Business Monitor-Implementierungsumgebung anhand der Schritte, die im übergeordneten Thema "Implementierungsumgebung mit einem Muster erstellen" beschrieben sind.

Als Nächstes installieren Sie entweder die IBM BPM-Widgets in IBM Business Monitor Business Space oder die IBM Business Monitor-Widgets in IBM BPM Business Space. Die erste Methode ist die einfachste und daher die bevorzugte Methode.

### IBM Business Process Manager-Widgets in IBM Business Monitor Business Space installieren

Zum Installieren von IBM Business Process Manager-Widgets in IBM Business Monitor Business Space installieren Sie die Widgets und registrieren anschließend die REST-Serviceendpunkte (REST = Representational State Transfer) bei den Widgets.

Führen Sie die folgenden Schritte aus, nachdem Sie die Implementierungsumgebung generiert haben:

1. Installieren Sie die IBM BPM Business Space-Widgets in der IBM Business Monitor-Implementierungsumgebung. Die Business Space-Widgets befinden sich im Stammverzeichnis von IBM BPM (beispielsweise IBM/BPM) /BusinessSpace/registryData/produktname/widgets. Wenn Sie nur die IBM BPM-Widgets installieren möchten, geben Sie für den Parameter **-widgets** als Wert *BPM\_installationsstammverzeichnis/BusinessSpace/registryData/BPM/widgets* an. Wenn Sie WebSphere Enterprise Service Bus-Widgets installieren möchten, geben Sie für den Parameter **-widgets** als Wert *WESB\_installationsstammverzeichnis/BusinessSpace/registryData/WESB/widgets* an. Beispiel:

```
AdminTask.installBusinessSpaceWidgets('[-clusterName clustername -widgets
installationsstammverzeichnis/BusinessSpace/registryData/BPM/widgets/]')
AdminTask.installBusinessSpaceWidgets('[-clusterName clustername -widgets
installationsstammverzeichnis/BusinessSpace/registryData/WESB/widgets/]')
```

2. Registrieren Sie die REST-Seerviceendpunkte bei den Widgets. Die REST-Services sind nur in den IBM BPM-Clustern verfügbar und müssen im IBM Business Monitor-Cluster registriert werden, damit die Widgets über den Business Space für IBM Business Monitor verwendet werden können.

Sie können die REST-Serviceendpunkte entweder in der Administrationskonsole oder in der Befehlszeile registrieren. Führen Sie die Anweisungen in der zugehörigen Task 'Mit der Administrationskonsole Business Space konfigurieren und REST-Endpunkte registrieren' bzw. 'REST-Service-Endpunkte für Business Space in der Befehlszeile registrieren' aus.

- Geben Sie für den Parameter **-clusterName** den Namen des IBM BPM-Clusters an, in dem die REST-Services installiert sind. Die IBM BPM-REST-Services können wahlweise in dem Anwendungscluster, auf dem Deployment Manager oder im Unterstützungscluster installiert werden. Stellen Sie sicher, dass Sie den richtigen Clusternamen auswählen.
- Geben Sie für den Parameter **-businessSpaceClusterName** den Cluster an, unter dem der Business Space für IBM Business Monitor installiert wurde.

In den folgenden Beispielen wird Jacl verwendet.

- Bei einer Einzelclusterumgebung:

```
$AdminTask registerRESTServiceEndpoint {-clusterName <#PS-clustername> -type "{com.ibm.bpm}BFM
```

- Bei einer Umgebung mit vier Clustern, in der IBM Business Monitor Business Space in dem Web-Cluster der Implementierungsumgebung installiert ist:

```
$AdminTask registerRESTServiceEndpoint {-clusterName WPSCluster.AppTarget -type "{com.ibm.bpm}
```

## IBM Business Monitor-Widgets in BPM Business Space installieren

Zum Installieren von IBM Business Monitor-Widgets in IBM Business Process Manager Business Space installieren Sie die Widgets, registrieren die REST-Serviceendpunkte (Representational State Transfer) bei den Widgets und führen die Endpunktconfiguration für die IBM Cognos Business Intelligence-Widgets aus.

Führen Sie die folgenden Schritte aus, nachdem Sie die Implementierungsumgebung generiert haben:

1. Installieren Sie die IBM Business Monitor Business Space-Widgets in der IBM BPM-Implementierungsumgebung.

```
AdminTask.installBusinessSpaceWidgets('[-clusterName clustername -widgets  
installationsstammverzeichnis/BusinessSpace/registryData/WBM/widgets/']')
```

2. Registrieren Sie die REST-Seerviceendpunkte bei den Widgets. Die REST-Services sind nur in den IBM BPM-Clustern verfügbar und müssen im IBM Business Monitor-Cluster registriert werden, damit die Widgets über den Business Space für IBM Business Monitor verwendet werden können.

Sie können die REST-Serviceendpunkte entweder in der Administrationskonsole oder in der Befehlszeile registrieren. Führen Sie die Anweisungen in der zugehörigen Task 'Mit der Administrationskonsole Business Space konfigurieren und REST-Endpunkte registrieren' bzw. 'REST-Service-Endpunkte für Business Space in der Befehlszeile registrieren' aus.

- Geben Sie für den Parameter **-clusterName** den Namen des IBM BPM-Clusters an, in dem die REST-Services installiert sind. Die IBM BPM-REST-Services können wahlweise in dem Anwendungscluster, auf dem Deployment Manager oder im Unterstützungscluster installiert werden. Stellen Sie sicher, dass Sie den richtigen Clusternamen auswählen.
- Geben Sie für den Parameter **-businessSpaceClusterName** den Cluster an, unter dem der Business Space für IBM Business Monitor installiert wurde.

In den folgenden Beispielen wird Jacl verwendet.

- Bei einer Einzelclusterumgebung:

```
$AdminTask registerRESTServiceEndpoint {-clusterName <WPS-clustername> -type "{com.ibm.bpm}
```

- Bei einer Umgebung mit vier Clustern, in der IBM Business Monitor Business Space in dem Web-Cluster der Implementierungsumgebung installiert ist:

```
$AdminTask registerRESTServiceEndpoint {-clusterName WPSCluster.AppTarget -type "{com.ibm.bpm}
```

3. Führen Sie die Serviceendpunktconfiguration der IBM Cognos BI-Widgets aus und gehen Sie dabei anhand der Anweisungen unter "IBM Business Monitor und Business Space für die Verwendung eines vorhandenen IBM Cognos BI-Service konfigurieren" vor.

---

## Die Implementierungsumgebung mithilfe einer benutzerdefinierte Topologie erstellen

Statt eines der bereitgestellten Implementierungsumgebungsmuster zu verwenden, können Sie eigene Cluster einrichten und die IBM Business Monitor-Komponenten in einer Network Deployment-Topologie konfigurieren.

Bevor Sie Cluster erstellen und die IBM Business Monitor-Komponenten konfigurieren, müssen Sie die folgenden Aufgaben ausgeführt haben:

- Sie haben IBM Business Monitor installiert.
- Sie haben das Deployment Manager-Profil für IBM Business Monitor erstellt oder ein vorhandenes Deployment Manager-Profil mit IBM Business Monitor erweitert.
- Sie haben die Monitor-Datenbank erstellt.
- Sie haben den Deployment Manager gestartet.
- Sie haben mindestens ein angepasstes IBM Business Monitor-Profil erstellt und eingebunden oder ein vorhandenes angepasstes Profil mit IBM Business Monitor erweitert.
- Sie haben das angepasste Profil bzw. die Profile gestartet.

Die folgenden Anweisungen beschreiben, wie Cluster erstellt, der CEI-Ereigniservice (Common Event Infrastructure) konfiguriert und die erforderlichen Komponenten mit dem Konfigurationsassistenten oder den wsadmin-Befehlen installiert und konfiguriert werden.

### IBM Business Monitor-Cluster erstellen

In einer Network Deployment-Umgebung müssen die IBM Business Monitor-Komponenten in Clustern implementiert werden.

Bevor Sie Cluster erstellen und die IBM Business Monitor-Komponenten konfigurieren, müssen Sie die folgenden Aufgaben ausgeführt haben:

- Sie haben IBM Business Monitor installiert.
- Sie haben das Deployment Manager-Profil für IBM Business Monitor erstellt oder ein vorhandenes Deployment Manager-Profil mit IBM Business Monitor erweitert.
- Sie haben die Monitor-Datenbank erstellt.
- Sie haben den Deployment Manager gestartet.
- Sie haben mindestens ein angepasstes IBM Business Monitor-Profil erstellt und eingebunden oder ein vorhandenes angepasstes Profil mit IBM Business Monitor erweitert.



- Sie haben das angepasste Profil bzw. die Profile gestartet.

Verwenden Sie zur Erstellung des ersten Cluster-Members ein vorhandenes angepasstes Profil. Sie können in den von Ihnen erstellten Clustern beliebig viele zusätzliche Cluster-Member hinzufügen. (Siehe "Cluster-Member hinzufügen"). Um den IBM Business Monitor-Cluster zu erstellen, führen Sie in der Administrationskonsole folgende Schritte aus:

1. Klicken Sie in der Navigationsanzeige auf **Server > Cluster > WebSphere Application Server-Cluster**.
2. Klicken Sie auf **Neu**, um den Assistenten zum Erstellen eines neuen Clusters zu starten.
3. Geben Sie einen Namen für den Cluster an.
4. Wählen Sie **Lokalen Knoten bevorzugen** aus, um die Weiterleitungsoptimierung im Hostbereich zu ermöglichen. Diese Einstellung verbessert die Leistungsdaten, da EJBs, soweit möglich, in einem Cluster-Member desselben Knotens gesucht werden.
5. Klicken Sie auf **Weiter**, um mit dem Schritt der Erstellung des ersten Cluster-Members fortzufahren.
6. Geben Sie einen Namen für das erste Cluster-Member an.
7. Geben Sie einen Knoten für das erste Cluster-Member an. Dieser Knoten muss ein IBM Business Monitor-Knoten sein.
8. Wählen Sie die Option **Member mit einer Anwendungsserverschablone erstellen** aus.
9. Wählen Sie eine Anwendungsservervorlage (in WAS: 'Anwendungsserverschablone') aus, die im Namen die Zeichenfolge *defaultWBM* enthält, und klicken Sie auf **Weiter**.

**Wichtig:** Wenn keine Vorlage mit dem Namensbestandteil 'defaultWBM' vorhanden ist, stellen Sie sicher, dass Sie einen Knoten ausgewählt haben, der mit IBM Business Monitor erweitert wurde.

Wenn das erste Cluster-Member nicht mit einer Anwendungsservervorlage mit dem Namensbestandteil 'defaultWBM' erstellt wird, wird Ihre IBM Business Monitor-Umgebung nicht ordnungsgemäß funktionieren und Sie müssen alle vorhandenen Cluster-Member löschen und das erste Cluster-Member erneut erstellen.

10. Klicken Sie auf **Weiter**, um mit dem Schritt der Erstellung weiterer Cluster-Member fortzufahren.
11. Optional: Führen Sie die folgenden Schritte für jedes Cluster-Member aus, um weitere Cluster-Member hinzuzufügen:
  - a. Geben Sie einen eindeutigen Namen für die zusätzlichen Member an. Der Name muss innerhalb des Knotens eindeutig sein.
  - b. Geben Sie einen Knoten für die zusätzlichen Cluster-Member an. Dieser Knoten muss ein IBM Business Monitor-Knoten sein.
  - c. Klicken Sie auf **Member hinzufügen**.
12. Klicken Sie auf **Weiter**, um zur Zusammenfassungsanzeige zu gelangen.
13. Überprüfen Sie die Daten, und klicken Sie auf **Fertig stellen**.
14. Klicken Sie auf **Speichern**, um die Änderungen an der Masterkonfiguration zu speichern.

Nach dem Erstellen eines Clusters können Sie jederzeit weitere Cluster-Member hinzufügen.



Wenn Sie einen Cluster nach der Installation des IBM Cognos Business Intelligence-Service zum ersten Mal starten, müssen Sie diesen Vorgang für jeden Server einzeln ausführen. Verwenden Sie nicht die Option 'ripplestart', weil diese Option IBM Cognos BI nicht genügend Zeit für die Initialisierung lässt.

An der Administrationskonsole werden möglicherweise Probleme gemeldet, wenn Sie den IBM Cognos Business Intelligence-Server zum ersten Mal starten. Die Initialisierung der einzelnen Serverinstanzen in der Content-Store-Datenbank von IBM Cognos Business Intelligence und im Plattenbereich während des ersten Starts benötigt erheblich mehr Zeit als ein normaler Start von IBM Cognos Business Intelligence.

### Cluster-Member hinzufügen

Sie können einem vorhandenen Cluster beliebig viele Cluster-Member hinzufügen.

**Wichtig:** Wenn das erste Cluster-Member nicht mit einer Anwendungsservervorlage mit dem Namensbestandteil 'defaultWBM' erstellt wird, wird Ihre IBM Business Monitor-Umgebung nicht ordnungsgemäß funktionieren und Sie müssen alle vorhandenen Cluster-Member löschen und das erste Cluster-Member erneut erstellen.

Führen Sie folgende Schritte aus, um zusätzliche Cluster-Member hinzuzufügen:

1. Klicken Sie in der Navigationsanzeige auf **Server > Cluster > WebSphere Application Server-Cluster > *clustername* > Cluster-Member**.
2. Klicken Sie auf **Neu**, um den Assistenten zum Erstellen neuer Cluster-Member zu starten.
3. Führen Sie für jedes neue Cluster-Member folgende Schritte aus:
  - a. Geben Sie einen eindeutigen Namen für die zusätzlichen Member an. Der Name muss innerhalb des Knotens eindeutig sein.
  - b. Geben Sie einen Knoten für die zusätzlichen Cluster-Member an. Dieser Knoten muss ein IBM Business Monitor-Knoten sein.
  - c. Klicken Sie auf **Member hinzufügen**.
4. Klicken Sie auf **Weiter**, um zur Zusammenfassungsanzeige zu gelangen.
5. Überprüfen Sie die Daten und klicken Sie auf **Fertig stellen**.
6. Klicken Sie auf **Speichern**, um die Änderungen an der Masterkonfiguration zu speichern.

**Anmerkung:** Während der IBM Business Monitor-Installation wird der Cognos-Service ebenfalls auf dem Knoten installiert und auf dem neuen Server konfiguriert, wenn ein Member zum Cluster hinzugefügt wird.

### Zusätzliche Knoten einbinden

Nach der Erstellung einer Umgebung mit hoher Verfügbarkeit in einer Network Deployment-Zelle, können Sie zu einem späteren Zeitpunkt zusätzliche Knoten in die Zelle einbinden, wenn dies erforderlich ist.

**Wichtig:** IBM Business Monitor bietet keine Unterstützung für portalbasierte Dashboards in derselben Zelle wie der IBM Business Monitor-Server v8.0.

Führen Sie für jeden einzelnen vorhandenen Knoten die folgenden Schritte aus, um die Knoten in den Deployment Manager einzubinden:

1. Starten Sie den Deployment Manager.

2. Führen Sie von dem Profilverzeichnis, das dem Knoten entspricht, den Sie einbinden möchten, den Befehl **addNode** aus und geben Sie dabei den Hostnamen des Deployment Managers und optional die Nummer des SOAP-Connector-Ports des Deployment Managers an.

```
profil-stammverzeichnis\bin\addNode.bat
hostname_des_deployment_managers [soap-port_des_deployment_managers]
profil-stammverzeichnis/bin/addNode.sh
hostname_des_deployment_managers [soap-port_des_deployment_managers]
```

Wenn Sie den Befehl mit aktivierter Tracefunktion ausführen wollen, dann verwenden Sie die Option `-trace`. Beispiel: `addNode hostname -trace`.

Weitere Details zur Ausführung des Befehls **addNode** finden Sie in den zugehörigen Informationen im Information Center für WebSphere Application Server.

## CEI-Ereignisservices konfigurieren

Bevor die IBM Business Monitor-Komponenten über die Administrationskonsole konfiguriert werden können, muss ein CEI-Ereignisservice (CEI = Common Event Infrastructure) in Ihrer Network Deployment-Zelle zur Verfügung stehen, den IBM Business Monitor zum Senden von Ereignissen verwenden kann. Derselbe CEI-Ereignisservice kann auch zum Empfangen von Ereignissen verwendet werden.

Wenn Sie ein eigenständiges Profil für IBM Business Monitor erstellt haben oder den Konfigurationsassistenten der Implementierungsumgebung verwendet haben, wurde bereits ein CEI-Ereignisservice für Sie erstellt. Wenn Sie IBM Business Monitor auf einer Process Server-Topologie hinzufügen, können Sie den CEI-Ereignisservice verwenden, der von Process Server für IBM Business Monitor implementiert wurde. Wenn dies nicht der Fall ist, befolgen Sie die Anweisungen auf dieser Seite, um einen neuen CEI-Ereignisservice zu erstellen.

Installieren Sie mithilfe des Befehls **wbmDeployCEIEventService** einen CEI-Ereignisservice auf einem Server oder Cluster und erstellen Sie die hierfür erforderlichen Ressourcen (Service Integration Bus und Messaging-Steuerkomponente). Zudem können Sie bei Bedarf die Zugriffsberechtigung konfigurieren und den Standarddatenspeicher des CEI-Ereignisservice aktivieren. (Der Ereignisservice-Datenspeicher wird für Produktionsumgebungen nicht empfohlen.) In der Kerntopologie für hohe Verfügbarkeit wird der CEI-Ereignisservice im Unterstützungscluster installiert.

Gehen Sie wie folgt vor, um einen neuen CEI-Ereignisservice zu installieren und zu konfigurieren:

1. Öffnen Sie eine Eingabeaufforderung und wechseln Sie in das Verzeichnis `bin` des Deployment Manager-Profiles (standardmäßig `DMGR01`), in dem WebSphere Application Server installiert ist, oder in einer Einzelserverumgebung in das Verzeichnis `bin` des eigenständiges Profils.
2. Starten Sie `wsadmin`, indem Sie folgenden Befehl ausführen:
  - `wsadmin.sh`
  - `wsadmin.bat`
3. Führen Sie den Befehl **wbmDeployCEIEventService** im Dialogbetrieb aus, indem Sie Folgendes in die Befehlszeile eingeben:

```
(jacc1) $AdminTask wbmDeployCEIEventService {-interactive}
(jython) AdminTask.wbmDeployCEIEventService('-interactive')
```

Alternativ können Sie den Befehl ausführen, indem Sie alle Parameter angeben. Ein Beispiel finden Sie unter "IBM Business Monitor-Komponenten mit `wsadmin`-Befehlen konfigurieren" über die zugehörigen Links.

4. Speichern Sie die Ergebnisse mithilfe des folgenden Befehls:
 

```
(jac1) $AdminConfig save
(jython) AdminConfig.save()
```
5. Um die Knoten zu synchronisieren, klicken Sie in der Administrationskonsole auf **Systemverwaltung > Knoten**, wählen Sie alle Knoten aus und klicken Sie auf **Vollständige Neusynchronisation**.
6. Führen Sie einen Neustart für den Deployment Manager aus, damit die CEI-Links in der Administrationskonsole angezeigt werden.

Der CEI-Ereignisservice ist aktiviert.

Eine vollständige Liste der Parameter sowie ein Beispiel finden Sie im Abschnitt zum IBM Business Monitor-CEI-Ereignisservice.

Wenn Sie den Datenspeicherschritt während der Ausführung von **wbmDeployCEIEventService** nicht durchgeführt haben, haben Sie die Möglichkeit, den Datenspeicher für den CEI-Ereignisservice später zu erstellen. Weitere Informationen hierzu finden Sie im Abschnitt "CEI-Datenbank konfigurieren".

## Umgebung mit dem Konfigurationsassistenten konfigurieren

Sie können die erforderliche IBM Business Monitor-Umgebung mithilfe des Konfigurationsassistenten in der Administrationskonsole konfigurieren.

Sie müssen folgende Tasks abgeschlossen haben:

- Mindestens ein angepasstes IBM Business Monitor-Profil wurde erstellt und eingebunden oder ein vorhandenes angepasstes Profil mit IBM Business Monitor (siehe 'Profile erstellen und erweitern') wurde erweitert.
- Mindestens ein Cluster mit der Anwendungsservervorlage defaultWBM wurde erstellt (siehe 'IBM Business Monitor-Cluster erstellen').
- Ein lokaler CEI-Ereignisservice (CEI = Common Event Infrastructure), den IBM Business Monitor zum Senden und Empfangen von Ereignissen verwenden kann, wurde konfiguriert (siehe 'CEI-Ereignisservices konfigurieren').

Stellen Sie vor dem Starten des Konfigurationsprozesses sicher, dass Sie Änderungen am Knoten automatisch synchronisieren (klicken Sie in der Administrationskonsole auf **Systemverwaltung > Konsoleinstellungen** und wählen Sie **Änderungen mit Knoten synchronisieren**) aus. Andernfalls müssen Sie die Änderungen nach jedem Hauptschritt manuell synchronisieren.

Die erforderlichen und optionalen Komponenten können über den Konfigurationsabschnitt 'IBM Business Monitor' der Administrationskonsole konfiguriert werden. Anweisungen zur manuellen Konfiguration sämtlicher IBM Business Monitor-Komponenten finden Sie in den zugehörigen Informationen. Dort finden Sie Links mit weiterführenden Taskinformationen.

1. Klicken Sie in der Navigationsanzeige auf **Server > IBM Business Monitor-Konfiguration**. Daraufhin erscheint eine Liste der erforderlichen und optionalen Komponenten. Überprüfen Sie den Status der einzelnen Komponenten. Wenn Sie über eine ND-Umgebung verfügen und keine Implementierungsumgebung konfiguriert haben, ist keine der Komponenten bereits installiert oder konfiguriert. In diesem Fall müssen Sie die nachfolgenden Schritte zur Installation und Konfiguration der Komponenten ausführen.
2. Führen Sie die folgenden Schritte aus, um den ausgehenden CEI-Ereignisservice zu konfigurieren. Der ausgehende CEI-Ereignisservice wird verwendet,

um Ereignisse, einschließlich Alerts, von IBM Business Monitor zu senden. Sie müssen eine Ereignis-Emitter-Factory konfigurieren, die auf den ausgehenden CEI-Ereignisservice verweist.

**Wichtig:** Bevor die Ereignis-Emitter-Factory konfiguriert werden kann, muss ein lokaler CEI-Service zur Verfügung stehen, den IBM Business Monitor zum Senden von Ereignissen verwenden kann. Anweisungen zur Erstellung eines lokalen CEI-Service finden Sie im Abschnitt „CEI-Ereignisservices konfigurieren“ auf Seite 142.

- a. Klicken Sie in der Liste der Komponenten auf **Ausgehender CEI-Ereignisservice**. Der Status des ausgehenden CEI-Ereignisservice und der Ereignis-Emitter-Factory wird angezeigt. Sofern bereits eine MonitorEmitterFactory existiert, enthält das Statusfeld den Namen des CEI-Ereignisservices, den die Emitter-Factory verwendet. Wenn die Emitter-Factory noch nicht konfiguriert wurde, wird die Nachricht 'Der lokale CEI-Ereignisservice ist vorhanden, jedoch ist die Ereignis-Emitter-Factory nicht vorhanden' angezeigt. In diesem Fall muss die Emitter-Factory erstellt und konfiguriert werden.
  - b. Wählen Sie unter **Ereignis-Emitter-Factory konfigurieren** den Server oder Cluster für die Ereignis-Emitter-Factory aus. Die Liste enthält alle verfügbaren Server und Cluster. Sie können ausschließlich Server auswählen, die über einen konfigurierten CEI-Ereignisservice verfügen. (Die verfügbaren Server und Cluster werden mit Stern (\*) angezeigt). Wenn Sie mehrere gleichnamige Server haben, vergewissern Sie sich, dass Sie den Server im richtigen Knoten auswählen.
  - c. Um den Konfigurationsassistenten zu starten, klicken Sie auf **Ereignis-Emitter-Factory konfigurieren**. Für die Zelle wird eine Emitter-Factory für ausgehende Ereignisse namens MonitorEmitterFactory erstellt. Das Statusfeld für den ausgehenden CEI-Ereignisservice enthält nun den von der MonitorEmitterFactory verwendeten CEI-Ereignisservice.
  - d. Wenn Sie zur Konfigurationsseite zurückkehren wollen, dann klicken Sie in der Hauptlinkliste auf **IBM Business Monitor-Konfiguration**.
3. Führen Sie die folgenden Schritte aus, um den Service Integration Bus zu erstellen und die Messaging-Steuerkomponente zu konfigurieren. Um Ereignisse überwachen zu können, benötigt IBM Business Monitor einen eigenen Bus sowie eine eigene Messaging-Steuerkomponente.

Wenn kein Bus vorhanden ist, wird einer für Sie erstellt, wenn Sie die Messaging-Steuerkomponente konfigurieren. Der Bus erhält die Bezeichnung MONITOR.<zellename>.Bus, die nicht geändert werden kann.

- a. Klicken Sie in der Liste der Komponenten auf **Messaging-Steuerkomponente**. Der Status für den Service Integration Bus und die Messaging-Steuerkomponente wird angezeigt.
- b. Um den Konfigurationsassistenten zu starten, klicken Sie auf **Messaging-Steuerkomponente konfigurieren**.
- c. Wählen Sie in der Anzeige **Bus-Member auswählen** eine der folgenden Optionen aus, um die Erstellungsposition der neuen Messaging-Steuerkomponente festzulegen, und klicken Sie auf **Weiter**:
  - **Cluster:** Wählen Sie diese Option aus, um die Messaging-Steuerkomponente in einem bestehenden Cluster zu erstellen. Sie müssen den Clusternamen in der Liste auswählen.
  - **Server:** Wählen Sie diese Option aus, um die Messaging-Steuerkomponente auf einem Server zu erstellen. Sie müssen den Server in der Liste auswählen. Wenn Sie mehrere gleichnamige Server haben, vergewissern Sie sich, dass Sie den Server im richtigen Knoten auswählen.

- d. Wählen Sie in der Anzeige **Typ des Nachrichtenspeichers auswählen** eine der folgenden Optionen aus und klicken Sie auf **Weiter**:
- **Datenspeicher**: Ein Datenspeicher ist ein Nachrichtenspeicher, der eine Reihe von Tabellen enthält, die für alle Member des Clusters, der die Messaging-Steuerkomponente betreibt, zugänglich sind.
  - **Dateispeicher**: Ein Dateispeicher ist ein Nachrichtenspeicher, der Dateien im Dateisystem über das Betriebssystem verwendet. Diese Option ist nicht verfügbar, wenn in der Anzeige **Bus-Member auswählen** die Option **Cluster** ausgewählt wurde.
- e. Wenn Sie einen Datenspeicher verwenden, müssen Sie in der Anzeige **Eigenschaften des Nachrichtenspeichers angeben** eine der folgenden Optionen auswählen:
- **Standarddatenquelle mit generiertem JNDI-Namen erstellen**: Standardmäßig verwendet der Datenspeicher Derby. Diese Option ist nicht verfügbar, wenn in der Anzeige **Bus-Member auswählen** die Option **Cluster** ausgewählt wurde.
  - **Vorhandene Datenquelle verwenden**: Bei Auswahl dieser Option müssen Sie die folgenden Felder ausfüllen:
    - **JNDI-Name der Datenquelle**: Wählen Sie den JNDI-Namen der Datenbank aus, die Sie einsetzen werden. Beispiel: jdbc/wbm/MonitorMEDatabase.
    - **Schemaname**: Geben Sie den Schemanamen ein. Beispiel: MONME00.
    - **Authentifizierungsalias**: Wählen Sie den Authentifizierungsalias aus, den Sie einsetzen werden. Sie müssen den Authentifizierungsalias auswählen, wenn die Tabellen erstellt werden sollen. Beispiel: Monitor\_JDBC\_Alias.
    - **Tabellen erstellen**: Wählen Sie diese Option aus, um die Tabellen in der Datenbank zu erstellen. Wenn Sie diese Option nicht auswählen, muss der Datenbankadministrator die Tabellen erstellen.
- f. Überprüfen Sie die Informationen in der Bestätigungsanzeige und klicken Sie auf **Fertig stellen**, um die Konfiguration abzuschließen. Die Statusfelder für den Bus und die Messaging-Steuerkomponente werden nun mit den neuen Konfigurationsdaten aktualisiert.
- Anmerkung:** Es kann einen Moment dauern, bis die Messaging-Steuerkomponente erfolgreich startet.
- g. Wenn Sie zur Konfigurationsseite zurückkehren wollen, dann klicken Sie in der Hauptlinkliste auf **IBM Business Monitor-Konfiguration**.
4. Stellen Sie sicher, dass der Bus und die Messaging-Steuerkomponente die korrekte Benutzer-ID für Ihre Umgebung enthalten:
- a. Klicken Sie in der Navigationsanzeige auf **Sicherheit > Bussicherheit**.
  - b. Klicken Sie auf den Bus für den IBM Business Monitor-Server. Die Seite 'Konfigurationseigenschaften' wird für den Bus angezeigt.
  - c. Klicken Sie unter 'Weitere Eigenschaften' auf **Sicherheit**. Eine weitere Eigenschaftenseite wird angezeigt.
  - d. Klicken Sie unter 'Authorization Policy' (Berechtigungsrichtlinie) auf **Benutzer und Gruppen in der Rolle "Bus-Connector"**.
  - e. Überprüfen Sie, ob Ihre Benutzer-ID existiert. Falls sie nicht existiert, führen Sie die folgenden Schritte aus, um sie hinzuzufügen:
    - 1) Klicken Sie auf **Neu**.



- 2) Wählen Sie **Benutzer** aus und geben Sie einen Filterwert ein, durch den Ihre Benutzer-ID gefunden wird. Klicken Sie auf **Weiter**.
- 3) Wählen Sie Ihre ID in der Liste aus und klicken Sie auf **Weiter**.
- 4) Überprüfen Sie die Änderungen und klicken Sie auf **Fertig stellen**.
- f. Wenn Sie zur Konfigurationsseite zurückkehren wollen, dann klicken Sie in der Hauptlinkliste auf **IBM Business Monitor-Konfiguration**.
5. Führen Sie die folgenden Schritte aus, um die Anwendung für die IBM Business Monitor-Aktionsservices zu installieren. Die Anwendung für die Aktionsservices ruft beim Empfang definierter Situationsereignisse, die von Monitor oder anderen Anwendungen ausgegeben wurden, Aktionen wie das Senden von Dashboard-Alerts oder E-Mail-Benachrichtigungen auf. Situationsereignisse weisen in der Regel auf Geschäftssituationen hin, auf die reagiert werden muss. Hierzu gehören z. B. das Fehlen von Papier in einem Drucker oder das Auftreten von Messwerten, die einen bestimmten Wert übersteigen.
  - a. Klicken Sie in der Liste der Komponenten auf **Aktionsservices**. Der Status der Anwendung wird angezeigt. Wenn die Anwendung ordnungsgemäß installiert ist, enthält das Statusfeld die Position der installierten Anwendung.
  - b. Wählen Sie in der Liste unter **Aktionsservices implementieren** den Server oder Cluster für die Anwendung für die Aktionsservices aus. Die Liste enthält alle verfügbaren Server und Cluster. Wählen Sie einen Server aus, auf dem IBM Business Monitor installiert ist. Wenn Sie mehrere gleichnamige Server haben, vergewissern Sie sich, dass Sie den Server im richtigen Knoten auswählen.
  - c. Klicken Sie auf **Aktionsservices implementieren**, um die Anwendung zu installieren. Die Anwendung wird installiert und das Gruppenprofil für Monitor-Aktionsservices erstellt. Das Statusfeld enthält nun die Position der installierten Anwendung mit dem Namen IBM\_WBM\_ACTIONSERVICES. Wurde die Anwendung in einem Cluster installiert, ist die Anwendung so lange nicht verfügbar, bis alle Knoten im Cluster synchronisiert wurden.
  - d. Wenn Sie zur Konfigurationsseite zurückkehren wollen, dann klicken Sie in der Hauptlinkliste auf **IBM Business Monitor-Konfiguration**.
6. Führen Sie die folgenden Schritte aus, um die Anwendung für geplante Monitor-Services zu installieren. Sie müssen diese Anwendung installieren, um eine zeitliche Planung der wiederholt ausgeführten Services vornehmen zu können. Zu diesen Services zählen unter anderem der Datenübertragungsservice und das KPI-Verlaufsprotokoll für Monitormodelle.
  - a. Klicken Sie in der Liste der Komponenten auf **Geplante Monitor-Services**. Der Status der Anwendung wird angezeigt. Wenn die Anwendung ordnungsgemäß installiert ist, enthält das Statusfeld die Position der installierten Anwendung.
  - b. Wählen Sie in der Liste unter **Geplante Monitor-Services implementieren** den Server oder Cluster für die Anwendung für geplante Monitor-Services aus. Die Liste enthält alle verfügbaren Server und Cluster. Wählen Sie einen Server aus, auf dem IBM Business Monitor installiert ist. Wenn Sie mehrere gleichnamige Server haben, vergewissern Sie sich, dass Sie den Server im richtigen Knoten auswählen.
  - c. Klicken Sie auf **Geplante Monitor-Services implementieren**, um die Anwendung zu installieren. Das Statusfeld enthält nun die Position der installierten Anwendung mit dem Namen IBM\_WBM\_DATA\_SERVICES. Wurde die Anwendung in einem Cluster installiert, ist die Anwendung so lange nicht verfügbar, bis alle Knoten im Cluster synchronisiert wurden.

- d. Wenn Sie zur Konfigurationsseite zurückkehren wollen, dann klicken Sie in der Hauptlinkliste auf **IBM Business Monitor-Konfiguration**.

Sie können die geplanten Services für jedes installierte Monitormodell anzeigen, indem Sie auf **Anwendungen > Monitor-Services > Geplante Monitor-Services** klicken.

7. Optional: Wenn Sie den IBM Cognos Business Intelligence-Service verwenden wollen, um eine mehrdimensionale Analyse auf Ihren Dashboards auszuführen, klicken Sie in der Liste der optionalen Komponenten auf **Cognos**. Der Status des Service wird angezeigt. Wenn der Service ordnungsgemäß installiert ist, enthält das Statusfeld die Position des installierten Service. (Wenn Sie IBM Cognos BI mit IBM Business Monitor installiert und ein eigenständiges Profil erstellt haben, dann ist der IBM Cognos BI-Service bereits implementiert.)
  - a. Zum Implementieren eines neuen IBM Cognos BI-Service müssen Sie den Server oder Cluster für den IBM Cognos BI-Service in der Liste auswählen. Die Liste enthält alle verfügbaren Server und Cluster. (Die verfügbaren Server und Cluster werden mit Stern (\*) angezeigt). Wenn Sie mehrere gleichnamige Server haben, vergewissern Sie sich, dass Sie den Server im richtigen Knoten auswählen.

Geben Sie einen Datenbanknamen ein, der für den Content-Store verwendet werden soll. Unter DB2 und Microsoft SQL Server darf der Datenbankname nicht mit dem Namen der Monitor-Datenbank übereinstimmen. Geben Sie einen Datenbankbenutzernamen und das zugehörige Kennwort an. Wenn Sie für den Content-Store und die Monitor-Datenbank den gleichen Benutzernamen verwenden, dann müssen Sie auch das gleiche Kennwort benutzen. Da der Datenbankbenutzer, der zum Zugriff auf die Content-Store-Datenbank angegeben wird, über die Berechtigung zum Erstellen von Tabellen in der Datenbank verfügen muss, wird empfohlen, einen neuen Datenbankbenutzer nur für die Content-Store-Datenbank zu erstellen.

**Anmerkung:** Der Benutzername und das Kennwort für die IBM Cognos BI-Content-Store-Datenbank werden in 'Cognos\_JDBC\_Alias' gespeichert. Dadurch ist es möglich, alle Berechtigungsnachweise für die Datenbank zentral zu verwalten. Wenn Sie den IBM Business Monitor IBM Cognos BI-Server starten, werden die aktuellen Werte an die IBM Cognos BI-Konfiguration übergeben, um IBM Cognos BI den Zugriff auf den Content-Store zu ermöglichen. Aufgrund dieser Integration können Sie den Benutzernamen und das Kennwort für den Content-Store mit der IBM Cognos BI-Konfigurationsanwendung nicht ändern.

Wenn die Verwaltungssicherheit aktiviert ist, müssen Sie außerdem den Benutzernamen des IBM Cognos BI-Administrators und das zugehörige Kennwort angeben.

Klicken Sie auf **Neuen Cognos-Service erstellen**. Das Statusfeld enthält nun die Position des installierten Service. Wurde dieser Service in einem Cluster installiert, wird der Service so lange als nicht verfügbar angezeigt, bis alle Knoten im Cluster synchronisiert und erneut gestartet wurden. Wenn die für die Implementierung benötigte Zeitdauer das Zeitlimit der Administrationskonsole für die Antwort überschreitet, dann wird möglicherweise eine Zeitlimitnachricht angezeigt. Warten Sie noch einige Minuten, bevor Sie versuchen, die Server erneut zu starten.

- b. Wenn auf Ihrem System bereits eine IBM Cognos BI-Version installiert ist, dann geben Sie unter **Bestehenden Cognos-Service verwenden** die URI des externen Dispatchers des IBM Cognos BI-Servers an. Sie finden diese URI im IBM Cognos BI-Konfigurationsclient in **Lokale Konfiguration >**



**Umgebung > Dispatcher-Einstellungen** (Beispiel: `http://my_host:my_port/p2pd/servlet/dispatch/ext`). Wenn die Verwaltungssicherheit auf dem IBM Cognos BI-Server aktiviert ist, müssen Sie auch den Benutzernamen und das Kennwort des IBM Cognos BI-Administrators angeben.

Klicken Sie auf **Bestehenden Cognos-Service verwenden**. Das Statusfeld enthält nun die Position des installierten Service.

- c. Wenn Sie zur Konfigurationsseite zurückkehren wollen, dann klicken Sie in der Hauptlinkliste auf **IBM Business Monitor-Konfiguration**.
8. Optional: Wenn Sie die IBM Business Monitor-Dashboards für mobile Geräte verwenden möchten, müssen Sie die folgenden Schritte ausführen, um die Anwendung zu installieren. Wenn Sie die Dashboards für mobile Geräte nicht verwenden möchten, müssen Sie die folgenden Schritte nicht ausführen.
- a. Klicken Sie in der Liste der optionalen Komponenten auf **Dashboards für mobile Geräte**. Der Status der Anwendung wird angezeigt. Wenn die Anwendung ordnungsgemäß installiert ist, enthält das Statusfeld die Position der installierten Anwendung.
  - b. Wählen Sie in der Liste unter **Dashboards für mobile Geräte implementieren** den Server oder Cluster für die Anwendung der Dashboards auf mobilen Geräten aus. Die Liste enthält alle verfügbaren Server und Cluster. Wählen Sie einen Server aus, auf dem IBM Business Monitor installiert ist. Wenn Sie mehrere gleichnamige Server haben, vergewissern Sie sich, dass Sie den Server im richtigen Knoten auswählen.
  - c. Klicken Sie auf **Dashboards für mobile Geräte implementieren**, um die Anwendung zu installieren. Das Statusfeld enthält nun die Position der installierten Anwendung mit dem Namen IBM\_WBM\_MOBILE\_DASHBOARD. Wurde die Anwendung in einem Cluster installiert, ist die Anwendung so lange nicht verfügbar, bis alle Knoten im Cluster synchronisiert wurden.
  - d. Wenn Sie zur Konfigurationsseite zurückkehren wollen, dann klicken Sie in der Hauptlinkliste auf **IBM Business Monitor-Konfiguration**.
9. Optional: Wenn Sie die Ereignis-Emitter-Services Java Messaging Service (JMS) und Representational State Transfer (REST) verwenden möchten, müssen Sie die folgenden Schritte ausführen, um die API-Serviceanwendung zu installieren. Anstatt Common Base Event direkt zu codieren oder zu generieren, können Sie dann diese Ereignis-Emitter-Services verwenden. Sie stellen die Ereignis-XML bereit, die Ereignis-Emitter-Services empfangen die Ereignis-XML und schließen diese in ein Common Base Event ein, sodass sie durch IBM Business Monitor verarbeitet werden kann.
- a. Klicken Sie in der Liste der optionalen Komponenten auf **Eingehende Ereignis-Emitter-Services (JMS und REST)**. Der Status der Anwendungen wird angezeigt. Wenn die Anwendungen ordnungsgemäß installiert sind, enthält das Statusfeld die Positionen der installierten Anwendungen.
  - b. Wählen Sie in der Liste unter **Ereignis-Emitter-Services implementieren** den Server oder Cluster für die Anwendungen aus. Die Liste enthält alle verfügbaren Server und Cluster. Wählen Sie einen Server aus, auf dem IBM Business Monitor installiert ist. Wenn Sie mehrere gleichnamige Server haben, vergewissern Sie sich, dass Sie den Server im richtigen Knoten auswählen.
  - c. Klicken Sie auf **Ereignis-Emitter-Services implementieren**, um die Anwendungen zu installieren. Das Anwendungsfeld enthält nun die Positionen der installierten Anwendungen. Wurden die Anwendungen in einem

Cluster installiert, sind die Anwendungen so lange nicht verfügbar, bis alle Knoten im Cluster synchronisiert wurden.

- d. Wenn Sie zur Konfigurationsseite zurückkehren wollen, dann klicken Sie in der Hauptlinkliste auf **IBM Business Monitor-Konfiguration**.
10. Optional: Führen Sie folgende Schritte aus, um das REST-Services-Gateway (REST = Representational State Transfer) für Widgets für Business Space zu konfigurieren.

**Anmerkung:** Da es sich bei dem REST-Services-Gateway um eine gemeinsam genutzte Komponente handelt, kann es nicht mit dem Konfigurationsassistenten konfiguriert werden. Wenn Sie Cluster mithilfe des Konfigurationsassistenten für Implementierungsumgebungen oder ein eigenständiges Profil erstellen, wird das REST-Services-Gateway für Sie konfiguriert. Das REST-Services-Gateway muss implementiert und in Business Space registriert sein, bevor Ihr Team die Widgets in Business Space verwenden kann.

- a. Klicken Sie in der Administrationskonsole auf **Server > Servertypen > WebSphere Application Server** oder auf **Server > Cluster > WebSphere Application Server-Cluster**.
  - b. Klicken Sie auf den Namen Ihres Servers oder Clusters.
  - c. Klicken Sie auf der Konfigurationsseite unter **Business Integration** auf **REST-Services**.
11. Optional: Führen Sie die folgenden Schritte aus, um Business Space zu konfigurieren.

**Anmerkung:** Da es sich bei dem Business Space um eine gemeinsam genutzte Komponente handelt, kann es nicht mit dem Konfigurationsassistenten konfiguriert werden. Wenn Sie Cluster mithilfe des Konfigurationsassistenten für Implementierungsumgebungen oder ein eigenständiges Profil erstellen, wird das Business Space für Sie konfiguriert.

- a. Klicken Sie in der Administrationskonsole auf **Server > Servertypen > WebSphere Application Server** oder auf **Server > Cluster > WebSphere Application Server-Cluster**.
  - b. Klicken Sie auf den Namen Ihres Servers oder Clusters.
  - c. Klicken Sie auf der Konfigurationsseite unter **Business Integration** auf **Business Space-Konfiguration**.
12. Nachdem Sie die Konfiguration der Komponenten abgeschlossen haben, synchronisieren Sie die Knoten. Klicken Sie in der Administrationskonsole auf **Systemverwaltung > Knoten**, wählen Sie alle Knoten aus und klicken Sie auf **Vollständige Neusynchronisation**. Stoppen Sie anschließend alle Cluster und Server und starten Sie sie erneut.

Melden Sie sich von der Administrationskonsole ab, um die ordnungsgemäße Installation und Konfiguration aller Anwendungen zu prüfen. Melden Sie sich anschließend bei der Administrationskonsole an und navigieren Sie zu **Server > IBM Business Monitor-Konfiguration**. Stellen Sie sicher, dass alle Einträge vollständig sind und ein grünes Häkchen aufweisen.

Wenn Sie die Erstellung der Tabellen der Messaging-Steuerkomponente nicht ausgewählt haben oder über keine Berechtigung zur Erstellung verfügen, müssen die Tabellen von einem Datenbankadministrator manuell erstellt werden. Weitere Informationen hierzu finden Sie im Abschnitt 'Tabellen für Messaging-Steuerkomponenten manuell erstellen' über die zugehörigen Links.

Wenn Sie Ereignisse von einer CEI-Ereignisquelle empfangen möchten, die sich auf einem fernen Server befindet, ist zudem die Durchführung einer zellenübergreifenden Konfiguration erforderlich. Anweisungen hierzu finden Sie im Abschnitt 'Empfang von Ereignissen konfigurieren'.

## Umgebung mithilfe von wsadmin-Befehlen konfigurieren

Anstatt den Konfigurationsassistenten zu verwenden, können Sie die IBM Business Monitor-Umgebung auch mithilfe des Befehlszeilenverwaltungstools von WebSphere (wsadmin) konfigurieren.

Die folgenden wsadmin-Befehle sind für die Konfiguration von IBM Business Monitor erforderlich.

*Tabelle 4. Erforderliche wsadmin-Befehle*

Befehl	Zweck
wbmDeployCEIEventService	Erstellt und konfiguriert den CEI-Ereignisservice, den IBM Business Monitor benötigt, um Ereignisse empfangen und senden zu können.
wbmConfigureEventEmitterFactory	Konfiguriert die Ereignis-Emitter-Factory, die IBM Business Monitor benötigt, um Ereignisse generieren und senden zu können. Dieser Befehl muss im Anschluss an den Befehl 'wbmDeployCEIEventService' ausgeführt werden.
wbmDeployMessagingEngine	Installiert und konfiguriert die für IBM Business Monitor erforderliche Messaging-Steuerkomponente und den Service Integration Bus.
wbmDeployActionServices	Installiert die IBM Business Monitor-Aktionsserviceanwendung. Diese Anwendung ruft beim Empfang definierter Situationsereignisse Aktionen wie das Senden von Dashboard-Alerts oder E-Mail-Benachrichtigungen auf. Dieser Befehl muss im Anschluss an den Befehl 'wbmConfigureEventEmitterFactory' ausgeführt werden.
wbmDeployScheduledServices	Installiert die Anwendung 'Geplante Monitor-Services', die wiederholt ausgeführte Services terminiert. Zu diesen Services zählen unter anderem der Datenübertragungsservice und das KPI-Verlaufsprotokoll für Monitormodelle.

Die Verwendung der folgenden wsadmin-Befehle ist optional.

*Tabelle 5. Optionale wsadmin-Befehle*

Befehl	Zweck
wbmDeployCognosService wbmSetCognosDispatcher	Installiert einen neuen IBM Cognos Business Intelligence-Service für die mehrdimensionale Analyse oder stellt eine Verbindung zu einem bereits vorhandenen IBM Cognos BI-Service her.

Tabelle 5. Optionale wsadmin-Befehle (Forts.)

Befehl	Zweck
wbmSetCognosDatabaseUser wbmSetCognosAdminUser	Ändert die Kennwörter für die Content-Store-Datenbank von IBM Cognos BI und den IBM Cognos BI-Administrator.
wbmRemoveCognosService	Entfernt den IBM Cognos BI-Service, der zusammen mit IBM Business Monitor installiert wurde.
wbmDeployDashboardsForMobileDevices	Installiert und konfiguriert die zum Ausführen der Dashboards für mobile Geräte erforderliche Anwendung.
wbmDeployEventEmitterServices	Installiert und konfiguriert die Serviceanwendungen REST-Ereignis-Emitter und JMS-Ereignis-Emitter. Der JMS-Ereignis-Emitter kann XML-Ereignisse asynchron an eine JMS-Warteschlange (JMS = Java Messaging Service) ohne den Common Base Event-Wrapper veröffentlichen, sodass XML-Ereignisse auch dann in die JMS-Warteschlange versetzt werden können, wenn die IBM Business Monitor-Services nicht verfügbar sind. Der REST-Ereignis-Emitter kann Ereignisse ohne den Common Base Event-Wrapper asynchron veröffentlichen. Sie definieren die XSD, welche die Struktur der Geschäftsinformationen beschreibt, und die REST-API generiert und sendet das Ereignis im für IBM Business Monitor korrekten Format.
wbmDeployBPMEmitterService	Installiert und konfiguriert die IBM Business Process Manager-Ereignisemitterdienstanwendung, die von IBM BPM verwendet werden soll.
wbmConfigureQueueBypassDatasource	Erstellt die Datenquelle, die zum Aktivieren der Warteschlangenumgehungskommunikation erforderlich ist, wenn IBM Business Monitor in einer anderen Zelle als der CEI-Server installiert ist.

Führen Sie die folgenden Schritte aus, um das wsadmin-Tool auszuführen:

- Öffnen Sie eine Eingabeaufforderung und wechseln Sie in das Verzeichnis bin des Deployment Manager-Profiles (standardmäßig DMGR01), in dem WebSphere Application Server installiert ist, oder in einer Einzelserverumgebung in das Verzeichnis bin des eigenständiges Profils.
- Starten Sie wsadmin, indem Sie einen der folgenden Befehle ausführen:
  - `wsadmin.sh -lang jacl -user <benutzername> -password <kennwort>`
  - `wsadmin.sh -lang jython -user <benutzername> -password <kennwort>`
  - `wsadmin.bat -lang jacl -user <benutzername> -password <kennwort>`
  - `wsadmin.bat -lang jython -user <benutzername> -password <kennwort>`
- Führen Sie die gewünschten Befehle aus. Im folgenden Beispiel wird Jacl zur Ausführung des Befehls 'wbmConfigureEventEmitterFactory' und zur anschließenden Speicherung der Änderungen verwendet:

```
$AdminTask wbmConfigureEventEmitterFactory {-cluster firstCluster}  
$AdminConfig save
```

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.wbmConfigureEventEmitterFactory('[-cluster firstCluster]')  
AdminConfig.save()
```

4. Speichern Sie die Änderungen nach der Ausführung der Befehle, bevor Sie wsadmin beenden. Verwenden Sie folgende Syntax, um die Änderungen zu speichern:

```
(jac1) $AdminConfig save  
(jython) AdminConfig.save()
```

5. In einer Network Deployment-Umgebung ist die Synchronisierung der Knoten erforderlich. Klicken Sie in der Administrationskonsole auf **Systemverwaltung** > **Knoten**, wählen Sie alle Knoten aus und klicken Sie auf **Vollständige Neusynchronisation**. Stoppen Sie anschließend alle Cluster und Server und starten Sie sie erneut.

## Dialogmodus

Wenn Sie einen Verwaltungsbefehl im Dialogmodus verwenden, wird bei der interaktiven Erfassung ihrer Eingabe eine Reihe von Schritten durchlaufen. Während dieses Prozesses wird ein textbasierter Assistent sowie eine ähnliche Funktionalität für den Benutzer des Assistenten in der Administrationskonsole bereitgestellt. Bei Verwendung des Parameters `-interactive` werden Sie dazu aufgefordert, die einzelnen Werte der Reihe nach einzugeben.

Die folgenden Beispiele veranschaulichen die Verwendung dieses Parameters.

```
(jac1) $AdminTask wbmConfigureEventEmitterFactory {-interactive}  
(jython) AdminTask.wbmConfigureEventEmitterFactory('-interactive')
```

Über den Befehl `help` erhalten Sie Hilfe zu jedem Verwaltungsbefehl.

```
(jac1) $AdminTask help wbmConfigureEventEmitterFactory  
(jython) print AdminTask.help ('wbmConfigureEventEmitterFactory')
```

Details zu den Befehlen und Befehlsparametern finden Sie im Abschnitt Konfigurationsbefehle (wsadmin).

Für Business Space-Befehle siehe Befehle (wsadmin-Scripterstellung) zur Konfiguration von Business Space.

## Umgebung manuell konfigurieren

Zum Konfigurieren der IBM Business Monitor-Umgebung sollte immer der IBM Business Monitor-Konfigurationsassistent oder der Konfigurationsassistent der Implementierungsumgebung verwendet werden. Diese Informationen zur manuellen Konfiguration können bei Erweiterungs- oder Fehlerbehebungsszenarios hilfreich sein.

### Ereignis-Emitter-Factory für IBM Business Monitor for z/OS konfigurieren

IBM Business Monitor erstellt und sendet Ereignisse über einen ausgehenden CEI-Ereignisservice. Der Ereignisservice wiederum verwendet eine zu konfigurierende Ereignis-Emitter-Factory. Es wird empfohlen, die Ereignis-Emitter-Factory mit dem IBM Business Monitor-Konfigurationsassistenten, dem Konfigurationsassistenten

für die Implementierungsumgebung oder mit der Task 'wsadmin' zu installieren. Ferner besteht die Möglichkeit, die Ereignis-Emitter-Factory manuell zu konfigurieren.

Führen Sie über die Administrationskonsole des Deployment Managers die folgenden Schritte aus:

1. Klicken Sie in der Navigationsanzeige auf **Serviceintegration > Common Event Infrastructure > Ereignis-Emitter-Factorys > Standard-CEI**.
2. Klicken Sie unter 'Weitere Eigenschaften' auf **Ereignisserviceübertragung**.
3. Wählen Sie Ihren Ereignisservice in der Liste **Ereignisservice** aus und klicken Sie dann auf **OK**.
4. Klicken Sie auf **Speichern**, um alle Änderungen an der Masterkonfiguration zu speichern.
5. Klicken Sie in der Navigationsanzeige auf **Serviceintegration > Common Event Infrastructure > Ereignis-Emitter-Factorys**.
6. Wählen Sie für **Bereich** die Option **Zelle** aus.
7. Klicken Sie auf **Neu**.
8. Geben Sie im Feld **Name** einen Factorynamen (*factoryname*) ein. Dabei ist *factoryname* ein beliebiger, von Ihnen gewählter Name. Beispiel: 'MonitorEmitterFactory'.
9. Geben Sie im Feld **JNDI-Name** den Wert `com/ibm/monitor/MonitorEmitterFactory` ein.
10. Gehen Sie bei **Ereignisübertragung** wie folgt vor:
  - a. Wählen Sie das Kontrollkästchen **Ereignisserviceübertragung unterstützen** aus.
  - b. Wählen Sie in der Liste im Feld **JNDI-Name für Ereignisserviceübertragung** den Eintrag **Einen der folgenden Einträge verwenden** aus.
  - c. Geben Sie im Eingabefeld unterhalb des Felds **JNDI-Name für Ereignisserviceübertragung** eine der folgenden Optionen ein:
    - Cluster: `cell/clusters/clustername/com/ibm/events/configuration/bus-transmission/Default`  
Dabei gilt Folgendes:  
*clustername* gibt den Cluster an, in dem die CEI implementiert ist.
    - Server: `cell/nodes/knotenname/servers/servername/com/ibm/events/configuration/bus-transmission/Default`  
Dabei gilt Folgendes:  
*knotenname* gibt den Knoten an, auf dem die CEI implementiert ist.  
*servername* gibt den Server an, auf dem die CEI implementiert ist.
11. Wählen Sie die Kontrollkästchen **Kompatibilitätsmodus mit früherem Protokoll für Ereignisserviceübertragung** ab.
12. Klicken Sie auf **OK** und anschließend auf **Speichern**, um die Änderungen in der Masterkonfiguration zu speichern.

### CEI-Datenbank konfigurieren

Sie können eine Common Event Infrastructure-Datenbank (CEI-Datenbank) manuell konfigurieren und die CEI-Funktionalität für IBM Business Monitor nutzen.

In diesem Abschnitt wird die Prozedur der Konfiguration einer CEI-Datenbank zur Verwendung mit IBM Business Monitor beschrieben.



IBM Business Monitor erfordert keine CEI-Datenbank. Eine solche Datenbank wird auch nicht empfohlen, weil sie bei der Verarbeitung von IBM Business Monitor-Ereignissen nicht effizient ist. Verwenden Sie stattdessen Aufzeichnungs- und Wiedergabeereignisse.

1. Führen Sie den entsprechenden Befehl aus, um den Datenspeicher für den CEI-Ereignisservice zu erstellen:
  - Befehl 'configEventServiceDB2DB'
  - Befehl 'configEventServiceDB2ZOSDB'
  - Befehl 'configEventServiceOracleDB'
  - Befehl 'configEventServiceSQLServerDB'

**Wichtig:** Erstellen Sie keinen Datenspeicher für den Ereignisservice für Produktionsumgebungen, weil die Leistung für die Speicherung von Ereignissen beeinträchtigt werden kann.

2. Speichern Sie nach der Generierung der Datenbankscripts Ihre Änderungen mit dem Befehl `$AdminConfig save`. Neben der Generierung der Datenbankscripts erstellen die Befehle auch JDBC-Ressourcen zur Verwendung durch den CEI-Ereignisservice.
3. Kopieren Sie die Scripts, die Sie generiert haben, auf den Datenbankserver. Die Verzeichnisposition für die Scripts hängt von dem Geltungsbereich ab, in dem CEI implementiert ist. Die Standardposition für die Scripts ist abhängig von dem Geltungsbereich ab, in dem CEI implementiert ist, eines der folgenden Verzeichnisse:

```
profil-stammverzeichnis/databases/event/clustername/dbscripts/  
datenbanktyp
```

```
profil-stammverzeichnis/databases/event/knotenname/servername/  
dbscripts/datenbanktyp
```

Dabei gilt Folgendes:

*profil-stammverzeichnis* ist das Profilverzeichnis für das Deployment Manager-Profil.

*clustername* ist der Cluster, in dem CEI implementiert ist.

*knotenname* ist der Knoten, in dem CEI implementiert ist.

*servername* ist der Server, auf dem CEI implementiert ist.

*datenbanktyp* ist das Verzeichnis für Ihre Datenbank, z. B. db2 oder oracle.

4. Melden Sie sich beim Datenbankserver als Benutzer mit Lese- und Schreibzugriff auf die Datenbank an. Öffnen Sie eine Eingabeaufforderung und initialisieren Sie die Befehlszeilenschnittstelle für die Datenbanksoftware. Zum Erstellen der Ereignisdatenbank führen Sie das Script für Ihren Datenbanktyp aus (z. B. `cr_event_db2 server db2-benutzer`).

Sie müssen außerdem die Tabellen der Messaging-Steuerkomponente für CEI erstellen. Informationen dazu finden Sie in 'Tabellen für Messaging-Steuerkomponenten manuell erstellen' unter den zugehörigen Links.

## Anwendung für IBM Business Monitor-Aktionsservices installieren

Die Anwendung für die IBM Business Monitor-Aktionsservices ruft beim Empfang definierter Situationsereignisse, die von IBM Business Monitor oder anderen Anwendungen ausgegeben wurden, Aktionen wie das Senden von Dashboard-Alerts oder E-Mail-Benachrichtigungen auf. Situationsereignisse weisen in der Regel auf



Geschäftssituationen hin, auf die reagiert werden muss. Hierzu gehören z. B. das Fehlen von Papier in einem Drucker oder das Auftreten von Messwerten, die einen bestimmten Wert übersteigen.

Vor der Installation von 'monactionmgr.ear' müssen Sie CEI und den Startup Beans Service auf dem Server aktivieren, auf dem Sie die Anwendung für Aktionsservices installieren wollen.

Führen Sie die folgenden Schritte aus, um die Anwendung für Aktionsservices über die Administrationskonsole zu installieren:

1. Klicken Sie in der Navigationsanzeige auf **Anwendungen > Anwendungstypen > WebSphere-Unternehmensanwendungen** aus.
2. Klicken Sie auf **Installieren**.
3. Wählen Sie für **Pfad der neuen Anwendung** eine der folgenden Optionen aus:
  - **Lokales Dateisystem:** Wählen Sie diese Option aus, wenn sich die Datei auf dem lokalen System befindet.
  - **Fernes Dateisystem:** Wählen Sie diese Option aus, wenn Sie über einen Web-Browser auf die Administrationskonsole auf einem anderen System zugreifen.
4. Klicken Sie auf **Durchsuchen**, suchen Sie die Datei 'monactionmgr.ear' und klicken Sie auf **Weiter**. Die EAR-Dateien befinden sich nach der Installation im folgenden Verzeichnis:

```
monitor_stammverzeichnis/installableApps.wbm
```

Dabei gilt Folgendes:

monitor\_stammverzeichnis steht für das Verzeichnis, in dem IBM Business Monitor installiert ist.

5. Klicken Sie in der Anzeige 'Installationsoptionen auswählen' auf **Weiter**.
6. Klicken Sie in der Anzeige 'Servern Module zuordnen' auf *servername* oder *clustername*, um das System anzugeben, auf dem die Anwendung installiert werden soll.
7. Wählen Sie die Kontrollkästchen für die Zeilen aus, die den einzelnen Modulen zugeordnet sind, und klicken Sie dann auf **Anwenden**.
8. Klicken Sie auf **Next** (Weiter).
9. Überprüfen Sie die Angaben in der Übersicht und klicken Sie auf **Fertig stellen**.

## Gruppenprofil für Monitor-Aktionsservices erstellen

Nachdem Sie die Anwendung für Monitor-Aktionsservices installiert haben, müssen Sie ein Ereignisgruppenprofil für den Empfang von Ereignissen erstellen.

Bevor Sie diese Task beginnen, müssen Sie die folgenden Tasks abgeschlossen haben:

- Anwendung für Monitor-Aktionsservices wurde installiert
- Common Event Infrastructure-Ereignisservices (CEI-Ereignisservice) für IBM Business Monitor wurden konfiguriert
- Deployment Manager wurde gestartet.

Führen Sie über die Administrationskonsole die folgenden Schritte aus, um das Ereignisgruppenprofil zu erstellen:

1. Klicken Sie in der Navigationsanzeige auf **Serviceintegration > Common Event Infrastructure > Ereignisservice**.
2. Klicken Sie unter 'Weitere Eigenschaften' auf **Ereignisservices**.

3. Klicken Sie auf die Option für den **Standard-CEI-Ereignisserver**.
4. Klicken Sie unter 'Weitere Eigenschaften' auf **Ereignisgruppen**.
5. Klicken Sie auf **Neu**.
6. Geben Sie für **Name der Ereignisgruppe** Action Services Group Profile ein.
7. Geben Sie im Feld **Zeichenfolge für Ereignisselektor** die Zeichenfolge `CommonBaseEvent[extendedDataElements/@name = 'BusinessSituationName']` ein.
8. Klicken Sie auf **Anwenden**.
9. Klicken Sie unter 'Weitere Eigenschaften' auf **Verteilerwarteschlangen**.
10. Klicken Sie auf **Neu**.
11. Wählen Sie in der Dropdown-Liste **JNDI-Name der Warteschlange** den Eintrag `jms/ActionManager/queue` aus.
12. Wählen Sie unter **JNDI-Name der Verbindungs-Factory für Warteschlangen** den Eintrag `jms/ActionManager/QueueConnFactory` aus.
13. Klicken Sie auf **Anwenden**.
14. Klicken Sie auf **Speichern**, um die Änderungen in der Masterkonfiguration zu speichern.

### Geplante Monitor-Services installieren

Die Anwendung für die geplanten Monitor-Services unterstützt mehrere Services, von denen einige zur Optimierung des Leistungsverhaltens oder zur Basisverarbeitung verwendet werden. Die Konfiguration erfolgt in der Administrationskonsole von WebSphere Application Server. Sie müssen diese Anwendung installieren, um eine zeitliche Planung der wiederholt ausgeführten Services vornehmen zu können. Zu diesen Services zählen unter anderem der Datenübertragungsservice und das KPI-Verlaufsprotokoll für Monitormodelle.

Führen Sie die folgenden Schritte aus, um die Anwendung für geplante Monitor-Services zu installieren:

1. Klicken Sie in der Navigationsanzeige auf **Anwendungen > Anwendungstypen > WebSphere-Unternehmensanwendungen** aus.
2. Klicken Sie auf **Installieren**.
3. Wählen Sie für **Pfad der neuen Anwendung** eine der folgenden Optionen aus:
  - **Lokales Dateisystem:** Wählen Sie diese Option aus, wenn sich die Datei auf dem lokalen System befindet.
  - **Fernes Dateisystem:** Wählen Sie diese Option aus, wenn Sie über einen Web-Browser auf die Administrationskonsole auf einem anderen System zugreifen.
4. Klicken Sie auf **Durchsuchen**, suchen Sie die Datei 'MonitorDataServices.ear' und klicken Sie auf **Weiter**. Die EAR-Dateien befinden sich nach der Installation im folgenden Verzeichnis:

```
monitor_stammverzeichnis/installableApps.wbm
```

Dabei gilt Folgendes:

monitor\_stammverzeichnis steht für das Verzeichnis, in dem IBM Business Monitor installiert ist.

5. Klicken Sie in der Anzeige 'Installationsoptionen auswählen' auf **Weiter**.
6. Klicken Sie in der Anzeige 'Servern Module zuordnen' auf *servername* oder *clustername*, um das System anzugeben, auf dem die Anwendung installiert werden soll.

7. Wählen Sie die Kontrollkästchen für die Zeilen aus, die den einzelnen Modulen zugeordnet sind, und klicken Sie dann auf **Anwenden**.
8. Klicken Sie auf **Next** (Weiter).
9. Überprüfen Sie die Angaben in der Übersicht und klicken Sie auf **Fertig stellen**.

In einer Network Deployment-Umgebung müssen Sie nach der Installation der Anwendung für geplante Monitor-Services eine Schedulerressource im selben Cluster erstellen. Befolgen Sie die Anweisungen in "Schedulerressource erstellen und konfigurieren".

### Schedulerressource erstellen und konfigurieren:

Eine Schedulerressource ist eine Komponente, die die Schedulerverarbeitung steuert, indem sie die Workload an den lokalen Work Manager delegiert, der während der Installation auf Zellenebene erstellt wurde. In einer eigenständigen Serverumgebung wird eine Schedulerressource für Sie während der Installation von IBM Business Monitor erstellt. In einer Network Deployment-Umgebung müssen Sie eine Schedulerressource auf demselben Server oder Cluster erstellen, auf dem sich auch die Datei 'MonitorDataServices.ear' befindet. In diesem Abschnitt werden die Schritte zum Erstellen einer Schedulerressource über die Administrationskonsole erläutert.

Sie müssen zuerst die geplanten Monitor-Services installieren, indem Sie die Anweisungen befolgen, die über den folgenden Link abgerufen werden können.

Nach der Installation der geplanten Services können Sie anhand der folgenden Schritte eine Schedulerressource für einen Server oder Cluster erstellen.

1. Klicken Sie in der Navigationsanzeige der Administrationskonsole auf **Ressourcen > Scheduler**.
2. Wählen Sie im Feld **Bereich** einen Server- oder Clusterbereich aus. Dieser Server oder Cluster muss mit dem Server oder Cluster übereinstimmen, der in der Datei 'MonitorDataServices.ear' aufgeführt ist.
3. Klicken Sie auf **Neu**.
4. Geben Sie im Feld **Name** den Namen ein, der für die Ressource angezeigt werden soll, z. B. 'DataServicesScheduler'.
5. Geben Sie im Feld **JNDI-Name** die Zeichenfolge sched/wbm/DataServicesScheduler ein.
6. Geben Sie eine Kurzbeschreibung dieser Schedulerressource ein.
7. Optional: Optional: Geben Sie eine Kategorie ein, die zum Klassifizieren oder Gruppieren der Ressource verwendet werden soll.
8. Wählen Sie im Feld **JNDI-Name der Datenquelle** die Zeichenfolge jdbc/wbm/MonitorDatabase aus.
9. Optional: Wählen Sie für den Aliasnamen der Datenquelle **Monitor\_JDBC\_Alias** aus.
10. Geben Sie im Feld **Tabellenpräfix** die Zeichenfolge des Präfix ein, das den Scheduler tabellen zugeordnet werden soll. Diese Angabe muss das Datenbankschema umfassen. Dieses Präfix ermöglicht die Unterscheidung der Scheduler und somit die gemeinsame Nutzung derselben Datenbank. In einer typischen Monitor-Umgebung sollte das Präfix mit dem Präfix übereinstimmen, das in der Monitor-Installations-DDL (<MONITOR\_SCHEMANAME>.MONSCHED\_) verwendet wurde. Beispiel: MONITOR.MONSCHED\_</MONITOR\_SCHEMANAME>.

11. Geben Sie im Feld **Abfrageintervall** die Anzahl der Sekunden an, die der Scheduler die Datenbank abfragen soll, um nach neuen Workloads zu suchen. Für IBM Business Monitor wird ein Wert zwischen 30 und 60 Sekunden empfohlen.
12. Wählen Sie im Feld **JNDI-Name für Work Manager** den Work Manager (**wm/wbm/DataServicesWorkManager**) aus.
13. Um die Verwaltungssicherheit zu aktivieren, sodass nur Administratoren über eine Zugriffsberechtigung verfügen, müssen Sie auf **Verwaltungsrollen verwenden** klicken.
14. Klicken Sie auf **OK**, um diese Schedulerressource zu speichern.

## Dashboards für mobile Geräte installieren

Sie können IBM Business Monitor-Dashboards auf mobilen Geräten verwenden. Sie müssen die Anwendung mit der Administrationskonsole von WebSphere Application Server installieren.

Führen Sie die folgenden Schritte aus, um die Anwendung für Dashboards für mobile Geräte zu installieren:

1. Klicken Sie in der Navigationsanzeige auf **Anwendungen > Anwendungstypen > WebSphere-Unternehmensanwendungen** aus.
2. Klicken Sie auf **Installieren**.
3. Wählen Sie für **Pfad der neuen Anwendung** eine der folgenden Optionen aus:
  - **Lokales Dateisystem:** Wählen Sie diese Option aus, wenn sich die Datei auf dem lokalen System befindet.
  - **Fernes Dateisystem:** Wählen Sie diese Option aus, wenn Sie über einen Web-Browser auf die Administrationskonsole auf einem anderen System zugreifen.
4. Klicken Sie auf **Durchsuchen**, suchen Sie die Datei 'MobileDashboard.ear' und klicken Sie auf **Weiter**. Die EAR-Dateien befinden sich nach der Installation im folgenden Verzeichnis:

```
monitor_stammverzeichnis/installableApps.wbm
```

Dabei gilt Folgendes:

`monitor_stammverzeichnis` steht für das Verzeichnis, in dem IBM Business Monitor installiert ist.

5. Klicken Sie in der Anzeige 'Installationsoptionen auswählen' auf **Weiter**.
6. Klicken Sie in der Anzeige 'Servern Module zuordnen' auf *servername* oder *clustername*, um das System anzugeben, auf dem die Anwendung installiert werden soll.
7. Wählen Sie die Kontrollkästchen für die Zeilen aus, die den einzelnen Modulen zugeordnet sind, und klicken Sie dann auf **Anwenden**.
8. Klicken Sie auf **Next** (Weiter).
9. Überprüfen Sie die Angaben in der Übersicht und klicken Sie auf **Fertig stellen**.

Nach der Installation der Anwendung sowie einiger Monitor-Modelle können Sie über die folgende Webadresse auf die Dashboards für mobile Geräte zugreifen:

```
http://hostname:portnummer/mobile
```

Dabei gilt Folgendes:

*hostname* steht für den vollständig qualifizierten Hostnamen oder die IP-Adresse des Servers, auf dem die Anwendung installiert ist.

*portnummer* steht für den Standardport, der für IBM Business Monitor-Anwendungen verwendet wird.

Damit die Dashboards ordnungsgemäß auf mobilen Geräten funktionieren, müssen Sie Business Space konfigurieren. Zum Konfigurieren von Business Space müssen Sie Tasks wie etwa das Aktivieren der Widgets und Konfigurieren von REST-Services abschließen.

## **Ereignis-Emitter-Services installieren**

Sie können die Ereignis-Emitter-Services, die Sie mit IBM Business Monitor verwenden möchten, manuell installieren. Vor der manuellen Installation von Ereignis-Emitter-Services ist zuerst die Erstellung von Ressourcen für die Ereignis-Emitter-Services erforderlich.

### **Ressourcen für manuell installierte Ereignis-Emitter-Services erstellen:**

Bei der manuellen Installation von Ereignis-Emitter-Services müssen zuerst Ressourcen erstellt werden. Wenn Sie die Emitter-Services nicht mithilfe des Konfigurationsassistenten installieren oder aus Leistungsgründen mehr als eine Instanz der Emitter-Services implementieren, müssen alle für die Ereignis-Emitter-Services erforderlichen Ressourcen manuell erstellt werden. Informationen hierzu erhalten Sie über die zugehörigen Links. Die erforderlichen Ressourcen werden über die Administrationskonsole von IBM Business Monitor erstellt.

Bevor Sie mit dieser Task beginnen, müssen Sie den Service Integration Bus (SIB) von IBM Business Monitor erstellen. Anweisungen hierzu finden Sie im zugehörigen Verweis.

Dieser Abschnitt enthält Anweisungen zur Erstellung der folgenden erforderlichen Ressourcen:

- JMS-Zielwarteschlange
- JMS-Fehlerzielwarteschlange
- Fehlerwarteschlangen-Verbindungsfactory
- Warteschlangenverbindungsfactory
- JMS-Warteschlange
- JMS-Fehlerwarteschlange
- Aktivierungsspezifikation
- Ereignis-Emitter-Factory für den REST-Ereignis-Emitter-Service
- Ereignis-Emitter-Factory für den JMS-Ereignis-Emitter-Service

**Anmerkung:** Wenn Sie diese Ressourcen für einen JMS-Emitter auf einem Server zum ersten Mal erstellen (wenn die Ereignisservices nicht zu einem früheren Zeitpunkt bereits manuell oder durch den Konfigurationsassistenten auf dem Server implementiert worden sind), können Sie alle Standardnamen verwenden, um die Installation der Emitter-Services zu vereinfachen. In den folgenden Schritten wird auf die Standardnamen hingewiesen. Sie können bereits definierte Ereignis-Emitter-Factorys wiederverwenden oder neue Ereignis-Emitter-Factorys erstellen. Erstellen Sie für REST und JMS separate Ereignis-Emitter-Factorys.

Erstellen Sie die Ressourcen über die Administrationskonsole von IBM Business Monitor und halten Sie dabei die vorgegebene Reihenfolge ein.

1. Führen Sie die folgenden Schritte aus, um die JMS-Zielwarteschlange zu erstellen:

- a. Wählen Sie **Service-Integration** > **Busse** aus und klicken Sie dann auf **MONITOR.zellenname.Bus**.
  - b. Wählen Sie **Destination resources (Empfängerressourcen)** > **Destinations (Empfänger)** und klicken Sie dann auf **Neu**.
  - c. Stellen Sie beim Start des Assistenten **create new destination queue creation** (Neue Zielwarteschlange erstellen) sicher, dass die Option **Queue** (Warteschlange) ausgewählt ist und klicken Sie auf **Weiter**.
  - d. Nennen Sie die Ressource *MonitorEventEmitterQueue2*. Der Standardname ist *MonitorEventEmitterQueue*.
  - e. Stellen Sie als Beschreibung eine allgemeine Beschreibung der Warteschlange bereit. Beispiel: *Warteschlange für die JMS-Ereignis-Emitter-Warteschlange des Business Monitor-Servers*. Klicken Sie auf **Next** (Weiter).
  - f. Wählen Sie den **Knoten** aus, auf dem sich das Busmember befindet, klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.
2. Wiederholen Sie Schritt 1 auf Seite 159, um die JMS-Fehlerzielwarteschlange zu erstellen. Nennen Sie die Ressource *MonitorEventEmitterErrorQueue2*. Der Standardname ist *MonitorEventEmitterErrorQueue*. Geben Sie als Beschreibung *Bus für die JMS-Ereignis-Emitter-Fehlerwarteschlange des Business Monitor-Servers* ein.
  3. Geben Sie die Fehlerwarteschlange als Ausnahmezielwarteschlange an.
    - a. Wählen Sie **Service-Integration** > **Busse** aus und klicken Sie dann auf **MONITOR.zellenname.Bus**.
    - b. Wählen Sie **Destination resources (Empfängerressourcen)** > **Destinations (Empfänger)** aus und wählen Sie die Zielwarteschlange aus, die Sie in Schritt 1 auf Seite 159 erstellt haben.
    - c. Wählen Sie im Abschnitt **Exception destination** (Ausnahmeziel) die Schaltfläche **Specify** (Angaben) und geben Sie den Namen der Fehlerwarteschlange an, die Sie in Schritt 2 erstellt haben.
    - d. Klicken Sie auf **OK** und anschließend auf **Speichern**.
  4. Führen Sie die folgenden Schritte aus, um die Fehlerwarteschlangen-Verbindungsfactory zu erstellen:
    - a. Wählen Sie **Ressourcen** > **JMS** > **Warteschlangenverbindungsfactorys** aus.
    - b. Wählen Sie den geeigneten Bereich für die neue Fehlerwarteschlangen-Verbindungsfactory aus und klicken Sie dann auf **Neu**.
    - c. Klicken Sie auf **OK**, um den Standard-Messaging-Provider zu akzeptieren.
    - d. Geben Sie auf der Registerkarte **Konfiguration Name, Beschreibung** und **JNDI-Name** für die neue Fehlerwarteschlangen-Verbindungsfactory ein und wählen Sie den **Busnamen** aus. Klicken Sie auf **OK** und anschließend auf **Speichern**. Beachten Sie hierzu folgende Listenelemente:
      - **Name:** *MonitorEmitterErrorQConnFactory2*
      - Standardname: *MonitorEmitterErrorQConnFactory*
      - **Beschreibung:** *ErrorQConnFactory für die JMS-Ereignis-Emitter-Warteschlange des Business Monitor-Servers*
      - **JNDI-Name:** *jms/MonitorEventEmitter/ErrorQConnFactory2*
      - Standard-JNDI-Name: *jms/MonitorEventEmitter/ErrorQConnFactory*
      - **Busname:** Wählen Sie die JMS-Fehlerzielwarteschlange aus, die Sie in Schritt 2 erstellt haben.



- e. Geben Sie die Sicherheitseinstellungen für eine geschützte Umgebung an und klicken Sie dann auf **Anwenden**. Der Authentifizierungsalias für die XA-Wiederherstellung ist *MonitorBusAuth*. Der containergesteuerte Authentifizierungsalias ist *MonitorBusAuth*.
5. Wiederholen Sie Schritt 4 auf Seite 160, um die Warteschlangenverbindungsfactory zu erstellen. Verwenden Sie folgende Angaben:
    - **Name:** *MonitorEmitterQConnFactory2*
    - Standardname: *MonitorEmitterQueueConnFactory*
    - **Beschreibung:** *QConnFactory für die JMS-Ereignis-Emitter-Warteschlange des Business Monitor-Servers*
    - **JNDI-Name:** *jms/MonitorEventEmitter/QueueConnFactory2*
    - Standard-JNDI-Name: *jms/MonitorEventEmitter/QueueConnFactory*
    - **Busname:** Wählen Sie die JMS-Zielwarteschlange aus, die Sie in Schritt 1 auf Seite 159 erstellt haben.
  6. Führen Sie die folgenden Schritte aus, um die JMS-Warteschlange zu erstellen:
    - a. Wählen Sie **Ressourcen > JMS > Queues (Warteschlangen)** aus.
    - b. Wählen Sie den geeigneten Bereich für die neue Warteschlange aus und klicken Sie auf **Neu**.
    - c. Klicken Sie auf **OK**, um den Standard-Messaging-Provider zu akzeptieren.
    - d. Geben Sie auf der Registerkarte **Konfiguration Name** und **JNDI-Name** für die neue Warteschlange ein und wählen Sie **Busname** und **Warteschlangennamenname** aus. Klicken Sie auf **Anwenden**. Beachten Sie hierzu folgende Listenelemente:
      - **Name:** *MonitorEventEmitterQueue2*
      - Standardname: *MonitorEventEmitterQueue*
      - **JNDI-Name:** *jms/MonitorEventEmitter/Queue2*
      - Standard-JNDI-Name: *jms/MonitorEventEmitter/Queue*
      - **Busname:** *MONITOR.zellenname.Bus*
      - **Warteschlangennamenname:** Wählen Sie die JMS-Zielwarteschlange aus, die Sie in Schritt 1 auf Seite 159 erstellt haben.
  7. Wiederholen Sie Schritt 6, um die JMS-Fehlerwarteschlange zu erstellen. . Verwenden Sie folgende Angaben:
    - **Name:** *MonitorEventEmitterErrorQueue2*
    - Standardname: *MonitorEventEmitterErrorQueue*
    - **JNDI-Name:** *jms/MonitorEventEmitter/ErrorQueue2*
    - Standard-JNDI-Name: *jms/MonitorEventEmitter/ErrorQueue*
    - **Busname:** *MONITOR.zellenname.Bus*
    - **Warteschlangennamenname:** Wählen Sie die JMS-Fehlerzielwarteschlange aus, die Sie in Schritt 2 auf Seite 160 erstellt haben.
  8. Führen Sie die folgenden Schritte aus, um die Aktivierungsspezifikation zu erstellen:
    - a. Wählen Sie **Ressourcen > JMS > Aktivierungsspezifikationen** aus.
    - b. Wählen Sie den geeigneten Bereich für die neue Aktivierungsspezifikation aus und klicken Sie auf **Neu**.
    - c. Klicken Sie auf **OK**, um den Standard-Messaging-Provider zu akzeptieren.



- d. Geben Sie auf der Registerkarte **Konfiguration Name** und **JNDI-Name** ein und wählen Sie **Busname**, **Destination type** (Zieltyp) und **Destination JNDI** (Ziel-JNDI) für die neue Aktivierungsspezifikation aus. Beachten Sie hierzu folgende Listenelemente:
  - **Name:** *MonitorEventEmitterActivationSpec2*
  - Standardname: *MonitorEventEmitterActivationSpec*
  - **JNDI-Name:** *jms/MonitorEventEmitter/ActivationSpec2*
  - Standard-JNDI-Name: *jms/MonitorEventEmitter/ActivationSpec*
  - **Busname:** *MONITOR.zellenname.Bus*
  - **Destination type** (Zieltyp): Warteschlange
  - **Destination JNDI** (Ziel-JNDI): Wählen Sie das JMS-Ziel aus, das Sie in Schritt 1 auf Seite 159 erstellt haben.
- e. Setzen Sie den **Authentication Alias** (Authentifizierungsalias) auf *MonitorBusAuth*. Klicken Sie auf **OK** und anschließend auf **Speichern**.
9. Führen Sie folgende Schritte durch, um die Ereignis-Emitter-Factory für den REST-Ereignis-Emitter-Service zu erstellen:
  - a. Wählen Sie **Serviceintegration** > **Common Event Infrastructure** > **Ereignis-Emitter-Factory**s aus.
  - b. Wählen Sie den geeigneten Bereich für die neue Ereignis-Emitter-Factory aus und klicken Sie auf **Neu**.
  - c. Geben Sie auf der Registerkarte **Konfiguration Name** und **JNDI-Name** für die neue Ereignis-Emitter-Factory ein. Klicken Sie auf **Anwenden**. Beachten Sie hierzu folgende Listenelemente:
    - **Name:** *EmitterFactoryForREST2*
    - Standardname: *EmitterFactoryForREST*
    - **JNDI-Name:** *com/ibm/monitor/EmitterFactoryForREST2*
    - Standard-JNDI-Name: *com/ibm/monitor/EmitterFactoryForREST*
  - d. Wählen Sie unter 'Ereignisübertragung' die Option **Ereignisserviceübertragung unterstützen** und **Einen der folgenden Einträge verwenden** aus und geben Sie dann *com/ibm/events/configuration/bus-transmission/Default* ein.
10. Wiederholen Sie Schritt 9, um die Ereignis-Emitter-Factory für den JMS-Ereignis-Emitter-Service zu erstellen. Klicken Sie auf **OK** und anschließend auf **Speichern**. Beachten Sie hierzu folgende Listenelemente:
  - **Name:** *EmitterFactory2*
  - JNDI-Name: *com/ibm/monitor/EmitterFactory2*
  - **Standardname:** *EmitterFactory*
  - Standard-JNDI-Name: *com/ibm/monitor/EmitterFactory*
11. Führen Sie einen Neustart Ihres Servers durch, um diese Änderungen zu aktivieren. Wenn Sie Ressourcen in einer Network Deployment-Umgebung erstellen, führen Sie einen Neustart des Clusters durch, in dem die Ressourcen erstellt wurden.

#### **Ereignis-Emitter-Services manuell installieren:**

Sie können die Ereignis-Emitter-Services, die Sie zusammen mit IBM Business Monitor verwenden, manuell installieren. Bei der manuellen Installation von Ereignis-Emitter-Services können Sie vorhandene Ressourcen verwenden oder Ressourcen für die Ereignis-Emitter-Services erstellen.

Wenn Sie sich entschließen, Ressourcen für die Ereignis-Emitter-Services zu erstellen, müssen Sie die Ressourcen erstellen, bevor Sie Ereignis-Emitter-Services manuell installieren. Anweisungen zum Erstellen von Ressourcen erhalten Sie über den zugehörigen Link.

**Anmerkung:** Sie erreichen in einer Network Deployment (ND)-Umgebung eine bessere Leistung, wenn Sie die Anwendung IBM\_WBM\_EMITTER\_SERVICES auf dem Server implementieren, auf dem der CEI-Ereignisservice (Common Event Infrastructure) installiert ist. Wenn Sie Cluster eingerichtet haben, implementieren Sie die Emitter-Services zusammen mit dem CEI-Ereignisservice im Unterstützungscluster.

Gehen Sie wie folgt vor, um die Ereignis-Emitter-Services manuell zu installieren:

1. Wählen Sie in der Administrationskonsole von IBM Business Monitor nacheinander **Anwendungen > Anwendungstypen > WebSphere-Unternehmensanwendungen** aus.

**Anmerkung:** Wenn Sie Ressourcen, wie im Abschnitt Ressourcen für manuell installierte Emitter-Services erstellen beschrieben, erstellt haben, denken Sie daran, den Server erneut zu starten, bevor Sie die Anwendung implementieren. Wenn Sie Ressourcen in einer ND-Umgebung erstellt haben, führen Sie einen Neustart des Clusters durch, in dem die Ressourcen erstellt wurden.

2. Klicken Sie auf **Installieren**.
3. Wählen Sie für **Pfad der neuen Anwendung** eine der folgenden Optionen aus:
  - **Lokales Dateisystem:** Wählen Sie diese Option aus, wenn sich die Datei auf dem lokalen System befindet.
  - **Fernes Dateisystem:** Wählen Sie diese Option aus, wenn Sie über einen Web-Browser auf die Administrationskonsole auf einem anderen System zugreifen.
4. Klicken Sie auf **Durchsuchen**, wählen Sie die Datei 'EmitterServices.ear' aus und klicken Sie auf **Weiter**. Die EAR-Dateien befinden sich nach der Installation im folgenden Verzeichnis:

```
monitor_stammverzeichnis/installableApps.wbm
```

Dabei gilt Folgendes:

monitor\_stammverzeichnis steht für das Verzeichnis, in dem IBM Business Monitor installiert ist.

5. Wählen Sie in der Anzeige 'Select installation options' (Installationsoptionen auswählen) die Option **Detailed** (Detailliert) aus und klicken Sie dann auf **Next** (Weiter). Klicken Sie in der nächsten Anzeige auf **Continue** (Fortsetzen).
6. Wenn die Emitter-Services-Anwendung bereits von einem Administrator oder mit dem Konfigurationsassistenten implementiert wurde, erstellen Sie einen eindeutigen Namen für Ihre Anwendung. Beispiel: *IBM\_WBM\_EMITTER\_SERVICES2*.
  - a. Klicken Sie in der Anzeige 'Map modules to servers' (Module Servern zuordnen) auf den *Server* oder *Cluster*, auf dem Sie die Anwendung installieren möchten.
7. Wählen Sie die Kontrollkästchen für die Zeilen aus, die den einzelnen Modulen zugeordnet sind, und klicken Sie dann auf **Anwenden**.
8. Klicken Sie auf **Next** (Weiter).

9. Optional: Wenn Sie selbst erstellte Ressourcen verwenden und die Standardwerte nicht akzeptieren möchten, müssen Sie Änderungen in der Anzeige 'Bind listeners for message-driven beans' (Listener für Message-driven Beans binden) vornehmen.
  - a. Geben Sie als **Activation Specification Target Resource JNDI name** (JNDI-Name der Zielressource für Aktivierungsspezifikation) den JNDI-Namen an, den Sie in Schritt 8 des Abschnitts Ressourcen für manuell installierte Emitter-Services erstellen festgelegt haben. Der Standardwert ist *jms/MonitorEventEmitter/ActivationSpec*.
  - b. Geben Sie als **Destination JNDI name** (JNDI-Name des Ziels) den JNDI-Namen der JMS-Warteschlange (nicht der Zielwarteschlange) an, den Sie in Schritt 6 des Abschnitts Ressourcen für manuell installierte Emitter-Services erstellen festgelegt haben. Der Standardwert ist *jms/MonitorEventEmitter/Queue*.
  - c. Setzen Sie **ActivationSpec authentication alias** (ActivateSpec-Authentifizierungsalias) auf **MonitorBusAuth**.
10. Optional: In der Anzeige 'Map resource references to resources' (Ressourcen Ressourcenverweise zuordnen) können Sie Ressourcen angeben, die Sie erstellt haben, oder die Standardwerte akzeptieren. Klicken Sie dann auf **Next** (Weiter).
  - a. Geben Sie als **Target Resource JNDI name for the EventEmitterMDB** (JNDI-Name der Zielressource für EventEmitterMDB) den JNDI-Namen an, den Sie in Schritt 9 des Abschnitts Ressourcen für manuell installierte Emitter-Services erstellen festgelegt haben; Sie können aber auch den Standardwert verwenden. Der Standardwert ist *com/ibm/monitor/EmitterFactory*.
  - b. Geben Sie als **Target Resource JNDI name for the EventEmitterREST** (JNDI-Name der Zielressource für EventEmitterREST) den JNDI-Namen an, den Sie in Schritt 9 des Abschnitts Ressourcen für manuell installierte Emitter-Services erstellen festgelegt haben; Sie können aber auch den Standardwert verwenden. Der Standardwert ist *com/ibm/monitor/EmitterFactoryForREST*.

**Anmerkung:** Nachdem Sie auf **Next** (Weiter) geklickt haben, wird möglicherweise folgende Nachricht angezeigt:

ADMA8019E: The resources that are assigned to the application are beyond the deployment target scope. Resources are within the deployment target scope if they are defined at the cell, node, server, or application level when the deployment target is a server, or at the cell, cluster, or application level when the deployment target is a cluster. Assign resource assignments that are within the deployment target scope of the application or confirm that these resource assignments are correct as specified.

Dies ist keine Fehlermeldung. Klicken Sie auf **Continue** (Fortsetzen).

11. Optional: Wenn die Emitter-Services-Anwendung bereits bei der Produktinstallation implementiert oder von einem Administrator manuell implementiert wurde, geben Sie dem zugeordneten Kontextstammverzeichnis dieser Anwendung einen eindeutigen Namen.
  - a. Geben Sie in der Anzeige 'Map context roots for web modules' (Kontextstammverzeichnisse für Webmodule zuordnen) */rest/bpm/events2* als Namen des zugeordneten Kontextstammverzeichnisses an. Der Standardwert ist */rest/bpm/events*.
12. Ordnen Sie in diesem Schritt Benutzer oder Gruppen der Rolle 'eventemitters' zu. Sie können auch alle authentifizierten Benutzer zuordnen, indem Sie die Rolle 'eventEmitters' auswählen und auf **Map special subjects** (Bestimmte

Subjekte zuordnen) und dann auf **All Authenticated in Application's realm** (Alle Authentifizierten im Anwendungsbereich) klicken.

- a. Wählen Sie in der Anzeige 'Map security roles to users or groups' (Sicherheitsrollen Benutzern oder Gruppen zuordnen) die Rolle **eventEmitters** aus, klicken Sie auf **Map special subjects** (Bestimmte Subjekte zuordnen) und klicken Sie dann auf **All Authenticated in Application's realm for a secure environment** (Alle Authentifizierten im Anwendungsbereich für eine sichere Umgebung). Wenn die Sicherheit nicht aktiviert ist, wählen Sie **Everyone** (Jeder) aus.
13. Überprüfen Sie die Angaben in der Übersicht und klicken Sie auf **Fertig stellen**.
14. Wählen Sie **Anwendungen > Unternehmensanwendungen > IBM\_WBM\_EMITTER\_REST\_SERVICES** aus und klicken Sie auf **Start**.

#### **Ereignis-Emitter-Services mithilfe des Konfigurationsassistenten installieren:**

Sie können die Ereignis-Emitter-Services für IBM Business Monitor mithilfe des Konfigurationsassistenten installieren. Weitere Informationen hierzu erhalten Sie über den zugehörigen Link.



---

## Kapitel 10. IBM Business Monitor-Komponenten konfigurieren

Nach der Installation von IBM Business Monitor können Sie weitere Komponenten konfigurieren.

---

### IBM Cognos BI konfigurieren

Um den IBM Cognos Business Intelligence-Service so einzurichten, dass er mehrdimensionale Analysen auf Ihren Dashboards durchführt, können Sie einen neuen IBM Cognos BI-Service konfigurieren, nachdem Sie IBM Business Monitor installiert haben, oder Sie können einen vorhandenen IBM Cognos BI-Service zur Verwendung mit IBM Business Monitor konfigurieren.

#### Neuen IBM Cognos BI-Service konfigurieren

Wenn Sie IBM Business Monitor installieren, können Sie optional auch den neuen IBM Cognos Business Intelligence-Service installieren. Sie können den neuen IBM Cognos BI-Service wie folgt konfigurieren: eine Implementierungsumgebung erstellen, den Konfigurationsassistenten über die Administrationskonsole ausführen, den Befehl **wbmDeployCognosService** verwenden oder ein eigenständiges IBM Business Monitor-Profil im Profile Management Tool erstellen. Sie müssen außerdem eine IBM Cognos BI-Datenbank und einen zugehörigen Benutzernamen für den Content-Store erstellen.

Bei der Erstellung oder Erweiterung eines Deployment Manager-Profiles oder eigenständigen Profils für IBM Business Monitor kopiert IBM Business Monitor Datenbanktreiber und Anwendungsdateien in die IBM Cognos BI-Installationsverzeichnisse. IBM Business Monitor erstellt außerdem die IBM Cognos BI-Unternehmensanwendung (EAR-Datei), damit sie für die Implementierung des IBM Cognos BI-Service verfügbar ist.

#### Clusteranforderungen

Für Cluster-Member ist mindestens 1 GB an zusätzlichem Plattenspeicherplatz für IBM Cognos BI erforderlich, weil auf jedem Cluster-Member eine Laufzeitinstanz erstellt werden muss.

Es ist wichtig, nur ein Cluster-Member auf einmal zu starten und dann abzuwarten, bis IBM Cognos BI vollständig initialisiert wurde, bevor das nächste Cluster-Member gestartet wird. IBM Cognos BI benötigt zusätzliche Zeit beim erstmaligen Start, denn die Laufzeitinstanz muss erstellt werden und die Content-Store-Datenbank muss initialisiert werden.

Der Start eines weiteren Cluster-Members vor der vollständigen Initialisierung der Content-Store-Datenbank kann eine Datenbankkorruption verursachen. Kommt es zur Datenbankkorruption, wird dies in der Protokolldatei `cogserver.log` für die IBM Cognos BI-Laufzeitinstanz vermerkt. Zur Systemwiederherstellung müssen Sie die Content-Store-Datenbank löschen, die Datenbank erneut erstellen und anschließend einen einzelnen Cluster-Member erneut starten. Das DDL-Script zur Datenbankerstellung befindet sich im Verzeichnis `/dbscripts/Cognos` im Deployment Manager.

## Datenbankanforderungen

Der IBM Cognos BI-Service benötigt für sein Content-Store-Repository eine extra Datenbank (standardmäßig als COGNOSCS-Datenbank bezeichnet). Sie können diese Datenbank während der Konfiguration eines eigenständigen Profils oder eines Deployment Manager-Profiles erstellen, das Datenbankentwurfstool (DbDesign-Generator) verwenden oder die Datenbank anhand der durch IBM Business Monitor bereitgestellten Scripts manuell erstellen.

Der IBM Cognos BI-Service erstellt Tabellen in der IBM Cognos BI-Content-Store-Datenbank, wenn diese das erste Mal erstellt wird. Da der Datenbankbenutzer, der zum Zugriff auf die Content-Store-Datenbank angegeben wird, über die Berechtigung zum Erstellen von Tabellen in der Datenbank verfügen muss, wird empfohlen, einen neuen Datenbankbenutzer nur für die Content-Store-Datenbank zu erstellen.

Auf Systemen, auf denen der IBM Cognos BI-Server ausgeführt wird, muss der Datenbankclient installiert sein. Die WebSphere-Umgebung muss auf den Client zugreifen können und der Client muss so konfiguriert werden, dass eine Verbindung zur Monitor-Datenbank hergestellt werden kann. Näheres hierzu finden Sie auf der Seite 'Hinweise zur Datenbankplanung' sowie in den Informationen für Ihre jeweilige Datenbank.

## Sicherheitsanforderungen

Wenn IBM Cognos BI das erste Mal implementiert wird, gehört die vorkonfigurierte Gruppe mit dem Namen 'Jeder' zu verschiedenen integrierten Gruppen und Rollen im IBM Cognos BI-Namensbereich. Hierzu gehört auch die Rolle Systemadministratoren. Sie müssen die Gruppe 'Jeder' aus allen integrierten Gruppen und Rollen entfernen und sie durch Gruppen, Rollen oder Benutzer ersetzen, die zur Beschränkung des Zugriffs auf die IBM Cognos BI-Software und -Verwaltung berechtigt sind.

Weitere Konfigurationseinstellungen finden Sie unter "IBM Cognos BI-Sicherheit konfigurieren".

Wenn IBM Cognos BI und Business Space nicht auf demselben Cluster-Member ausgeführt werden, müssen Sie den Hostnamen und die Portnummer für IBM Cognos BI zur Liste der vertrauenswürdigen Server in IBM Cognos BI hinzufügen. Andernfalls können Sie die Seiten in Business Space nicht anzeigen. Informationen hierzu finden Sie im Schritt 3 auf Seite 173 im Thema "IBM Business Monitor und Business Space für die Verwendung eines vorhandenen IBM Cognos BI-Service konfigurieren."

## IBM Cognos BI-Systemkompatibilität

Wenn Sie ein Deployment Manager-Profil für IBM Business Monitor erstellen oder erweitern, werden die Konfigurationsdateien kopiert und eine EAR-Datei (EAR = Enterprise Archive) für IBM Cognos BI generiert. Die IBM Cognos BI-EAR-Datei wird speziell für die jeweilige Plattformarchitektur (Betriebssystem und Bitmodus) erstellt. Wenn IBM Business Monitor den IBM Cognos BI-Service implementiert, wird die EAR-Datei verwendet, die auf dem Deployment Manager für alle Knoten in der Zelle generiert wurde, die IBM Cognos BI ausführen. Damit die EAR-Datei erfolgreich ausgeführt werden kann, müssen alle Knoten denselben Typ aufweisen. Liegen Knoten vor, deren Typ vom Typ des Deployment Managers abweicht, müssen Sie eine EAR-Datei auf einem der Knoten generieren. Siehe "EAR-Datei für



IBM Cognos BI auf einem angepassten IBM Business Monitor-Knoten generieren".

## Bitmodi

Alle IBM Cognos BI-Server sind zur Ausführung im gleichen Bitmodus wie der Deployment Manager konfiguriert. Wenn der Deployment Manager z. B. auf einer 32-Bit-Plattform ausgeführt wird, dann sind alle IBM Cognos BI-Server im 32-Bit-Modus konfiguriert.

Wenn Sie den Bitmodus ändern wollen, dann müssen Sie für jeden IBM Cognos BI-Server die folgenden Schritte ausführen:

1. Klicken Sie in der Administrationskonsole auf **Server > Servertypen > Web-Sphere Application Server > servername**. Die Anzeige 'Konfiguration' wird angezeigt.
2. Erweitern Sie unter 'Serverinfrastruktur' die Sicht des Eintrags **Java- und Prozessverwaltung** und klicken Sie auf **Prozessdefinition**.
3. Klicken Sie unter 'Weitere Eigenschaften' auf **Umgebungseinträge**. Klicken Sie für jeden Server auf **PATH** (Pfad) und aktualisieren Sie die Pfadeinstellungen für die Umgebungsvariablen, sodass auf das korrekte Verzeichnis verwiesen wird. Bei 32-Bit-Systemen müssen Sie auf das Verzeichnis bin verweisen. Bei 64-Bit-Systemen muss hingegen auf das Verzeichnis bin64 verwiesen werden.
4. Synchronisieren Sie den Knoten und führen Sie für den Server einen Neustart durch.

## Laufzeitstammverzeichnis für IBM Cognos BI finden

Da die IBM Cognos BI-Konfigurationseinstellungen und -Binärdateien nur für eine einzige Laufzeitinstanz verwendet werden, muss IBM Business Monitor möglicherweise bei der Implementierung des Service eine neue Kopie für jede Laufzeitinstanz erstellen. Beim Start prüft IBM Business Monitor, ob an der Basisinstallation von IBM Cognos BI Aktualisierungen vorgenommen wurden, und wendet diese auf die Kopie für jede Laufzeitinstanz an. Wenn Änderungen an IBM Cognos BI erforderlich sind, muss daher nur die Basisinstallation aktualisiert werden.

Die Kopie für jede Laufzeitinstanz wird unter das Profil gestellt, das den IBM Cognos BI-Service ausführt. Alle Konfigurationsdateien, Laufzeitbinärdateien und Protokolldateien für jede Laufzeitinstanz werden in eindeutigen Verzeichnissen verwaltet. Die folgende Tabelle zeigt die Position des IBM Cognos BI-Stammverzeichnisses für die IBM Cognos BI-Laufzeitinstanz:

Tabelle 6. Position des IBM Cognos BI-Stammverzeichnisses

Servertyp	Verzeichnis
Erster eigenständiger Server	application_server-stammverzeichnis/ cognos
Zweiter eigenständiger Server	profil-stammverzeichnis/profilname/ cognos/servername
Cluster-Member-Server	profil-stammverzeichnis/profilname/ cognos/servername

## IBM Cognos BI-Konfiguration aktualisieren

IBM Business Monitor speichert Aktualisierungen an der IBM Cognos BI-Konfiguration bei jeder Ausführung des AdminTask-Befehls **wbmDeployCognosService**. An-

dert sich beispielsweise die Sicherheitseinstellung von eingebunden in eigenständiges LDAP oder ändern sich die Datenbankeinstellungen von Content Manager, führen Sie den Befehl **wbmDeployCognosService** aus, um IBM Cognos BI auf der Basis der Parameter, die Sie an den Befehl übergeben, sowie der aktuellen WebSphere-Einstellungen für die Datenbank und Benutzerregistry zu rekonfigurieren.

Die Änderungen an der Laufzeitinstanz der IBM Cognos BI-Konfiguration werden während des Serverstarts auf der Basis der Änderungen von **wbmDeployCognosService** vorgenommen. IBM Business Monitor prüft bei jedem Serverstart auf Änderungen an der IBM Cognos BI-Konfiguration.

Führen Sie den Befehl **wbmDeployCognosService** für die folgenden Typen von Änderungen an WebSphere aus:

- Änderungen an der Benutzerregistry
- Datenbankänderungen an IBM Business Monitor oder an IBM Cognos BI
- Änderungen des Hostnamens, der IP-Adresse und der HTTP-Portadresse

**Wichtig:** In der IBM Cognos BI-Konfiguration über den Befehl **wbmDeployCognosService** vorgenommene Aktualisierungen werden ignoriert, wenn mit der IBM Cognos BI-Konfigurationsanwendung bereits manuelle Konfigurationsänderungen getätigt wurden. Sobald Sie die IBM Cognos BI-Konfigurationsanwendung einmal verwendet haben, müssen Sie sie auch weiterhin für Änderungen verwenden.

Führen Sie den Befehl **wbmSetCognosDatabaseUser** für die folgenden Typen von Änderungen aus (oder bearbeiten Sie den WebSphere-Autorisierungsalias Cognos\_JDBC\_Alias direkt):

- Benutzername oder Kennwort für die IBM Cognos BI-Content-Store-Datenbank

Führen Sie den Befehl **wbmSetCognosAdminUser** für die folgenden Typen von Änderungen aus (oder bearbeiten Sie den WebSphere-Autorisierungsalias Cognos\_Admin\_Alias direkt):

- Benutzername oder Kennwort für den IBM Cognos BI-Benutzer mit Verwaltungsaufgaben

## IBM Cognos BI-Konfiguration manuell aktualisieren

Wenn die in IBM Business Monitor vorkonfigurierten Konfigurationseinstellungen für IBM Cognos BI für komplexe Konfigurationen nicht ausreichen, müssen Sie IBM Cognos BI mit der IBM Cognos BI-Konfigurationsanwendung manuell konfigurieren. Verwenden Sie die IBM Cognos BI-Konfigurationsanwendung, um gültige Domänennamen bzw. Hosteinstellungen der IBM Cognos BI-Firewalleinstellungen für die Host- und Portadressen der Systeme festzulegen, auf denen Business Space aktiv ist.

Für jede eindeutige Konfiguration ist ein eindeutiges Startscript vorhanden:

-  cogconfig.bat
-   cogconfig.sh




Das Script befindet sich in einem der folgenden Verzeichnisse:

- *cognos-installationsstammverzeichnis/bin* für 32-Bit-Server
- *cognos-installationsstammverzeichnis/bin64* für 64-Bit-Server

Verwenden Sie die obige Tabelle, um das Verzeichnis *cognos-installationsstammverzeichnis* zu finden.

Für jede eindeutige Konfiguration ist ein eindeutiges Startscript vorhanden: *cogconfig.bat* oder *cogconfig.sh* im Verzeichnis *cognos-installationsstammverzeichnis/bin* für 32-Bit-Server oder im Verzeichnis *cognos-installationsstammverzeichnis/bin64* für 64-Bit-Server. Verwenden Sie die obige Tabelle, um das Verzeichnis *cognos-installationsstammverzeichnis* zu finden.

Falls beim Starten des Scripts ein Problem auftritt, weil Java nicht gefunden wird, führen Sie einen ähnlichen Befehl wie den folgenden aus, um die Umgebung so festzulegen, dass die mit Ihrem WebSphere-Server verwendete Java-Version lokalisiert wird:

-  `SET JAVA_HOME=C:\WAS70\java`
-   `export JAVA_HOME=/opt/IBM/WebSphere/AppServer/java`

**Wichtig:** Führen Sie die IBM Cognos BI-Konfigurationsanwendung erst aus, nachdem der IBM Cognos BI-Server mindestens einmal gestartet wurde. Beim ersten Start wird die Konfiguration kopiert. (Zudem werden die Binärdateien kopiert, wenn nicht der erste eigenständige Server gestartet wird.) Darüber hinaus werden die Verschlüsselungsschlüssel erstellt und die Kennwörter innerhalb der Konfiguration verschlüsselt.

**Tip:** Nachdem die IBM Cognos BI-Konfiguration mit der IBM Cognos BI-Konfigurationsanwendung gespeichert wurde, prüft IBM Business Monitor nicht mehr auf Änderungen an der IBM Cognos BI-Konfiguration. IBM Business Monitor aktualisiert jedoch weiterhin die Benutzernamen und Kennwörter, sodass Sie Änderungen an diesen nur an einer Stelle vornehmen müssen (beispielsweise mit der WebSphere-Administrationskonsole, um den Autorisierungsalias zu ändern). IBM Business Monitor aktualisiert die IBM Cognos BI-Konfiguration beim Serverstart mit dem Namen und Kennwort aus dem WebSphere-Sicherheitsalias **Cognos\_JDBC\_Alias**. Wenn Sie das eigenständige WebSphere-LDAP-Repository verwenden, werden Änderungen am LDAP-Zugriff in der IBM Cognos BI-Konfiguration aktualisiert.

Wenn Sie den IBM Cognos-Verwaltungsclient verwenden müssen, finden Sie diesen unter `http://hostname:portnummer/p2pd/servlet/dispatch/ext`.

## Von IBM Business Monitor verwendete IBM Cognos BI-Adresse manuell festlegen

Verwenden Sie den Befehl **wbmSetCognosDispatcher**, um die Adresse eines fernen oder eines vorhandenen IBM Cognos BI-Service festzulegen oder um die Adresse eines lokal installierten IBM Cognos BI-Service zu ändern. Zur Unterstützung von Single Sign-on für Interaktionen zwischen IBM Cognos BI und IBM Business Monitor sollte die IBM Cognos BI-Adresse mit `/ext` enden (die vollständige Adresse des externen Dispatchers von IBM Cognos BI).

Starten Sie alle IBM Business Monitor-Server erneut, nachdem Sie die Adresse geändert haben.

## EAR-Datei für IBM Cognos BI auf einem angepassten IBM Business Monitor-Knoten generieren

Wenn Sie ein Deployment Manager-Profil für IBM Business Monitor erstellen oder erweitern, wird eine EAR-Datei (EAR = Enterprise Archive) für IBM Cognos Business Intelligence speziell für das jeweilige Betriebssystem und den jeweiligen Bitmodus generiert. Damit die EAR-Datei erfolgreich ausgeführt werden kann, müssen alle Knoten denselben Typ aufweisen. Liegen Knoten vor, deren Typ vom Typ des Deployment Managers abweicht, müssen Sie eine EAR-Datei auf einem der Knoten generieren.

Führen Sie folgende Schritte aus, um eine EAR-Datei auf einem angepassten IBM Business Monitor-Knoten zu generieren:

1. Kopieren Sie die folgenden Dateien aus IBM Business Monitor-Verzeichnissen in die IBM Cognos BI-Installationsverzeichnisse.

**Wichtig:** Sie müssen einige der Dateien (wie in der Tabelle angegeben) umbenennen, um vorhandene Dateien zu ersetzen.

Kopierquelle (Position und Dateiname)	Kopierziel (Position und Dateiname)
application_server-stammverzeichnis/ scripts.wbm/cognos/application.xml	application_server-stammverzeichnis/ cognos/war/p2pd/application.xml.template
application_server-stammverzeichnis/ scripts.wbm/cognos/web.xml	application_server-stammverzeichnis/ cognos/webapps/p2pd/WEB-INF/ web.xml.withCM
application_server-stammverzeichnis/ scripts.wbm/cognos/ibm-web-ext.xmi	application_server-stammverzeichnis/ cognos/webapps/p2pd/WEB-INF/ibm-web- ext.xmi
application_server-stammverzeichnis/ installableApps.wbm/monAuthProvider.jar	application_server-stammverzeichnis/ cognos/webapps/p2pd/WEB-INF/lib/ monAuthProvider.jar

2. Öffnen Sie eine Eingabeaufforderung in application\_server-stammverzeichnis/  
cognos/war/p2pd.
3. Führen Sie den folgenden Befehl aus:

 build.bat ear

  build.sh ear

Mit diesem Befehl wird eine WebSphere-EAR-Datei mit dem Namen p2pd.ear im IBM Cognos BI-Stammverzeichnis erstellt. Die Erstellung der EAR-Datei kann einige Minuten in Anspruch nehmen.

4. Kopieren Sie die neue Datei p2pd.ear in den Deployment Manager und ersetzen Sie dabei die vorhandene Datei in application\_server-stammverzeichnis/  
cognos.
5. Implementieren Sie den IBM Cognos BI-Service.

## IBM Business Monitor und Business Space für die Verwendung eines vorhandenen IBM Cognos BI-Service konfigurieren

Wenn auf Ihrem System IBM Cognos Business Intelligence bereits installiert ist, dann können Sie den vorhandenen IBM Cognos BI-Service mit IBM Business Monitor verwenden. Sie können eine Verbindung zu Ihrem vorhandenen IBM Cognos BI-Service auf die folgenden Arten herstellen: Ausführen des Konfigurationsassistenten von IBM Business Monitor über die Administrationskonsole, Verwenden des

Befehls **wbmSetCognosDispatcher** oder Erstellen eines eigenständigen Profils im Profile Management Tool. Anschließend müssen Sie bestimmte Konfigurationstasks ausführen.

Nachdem Sie eine Verbindung zwischen IBM Business Monitor und dem IBM Cognos BI-Server hergestellt haben, müssen Sie weitere Schritte ausführen, um Business Space einzurichten und Ihre Datenservices zu verwalten.

**Wichtig:** Das ferne IBM Cognos BI-System muss auf einem WebSphere Application-Server ausgeführt werden. Wenn die Verwaltungssicherheit aktiviert ist, dann muss das Benutzerrepository auf dem IBM Business Monitor-Server und dem Benutzerrepository auf dem IBM Cognos BI-Server identisch sein.

Stellen Sie sicher, dass der Datenbankclient aktiv ist und auf die IBM Business Monitor-Datenbank auf dem fernen IBM Cognos BI-Server zugreifen kann. Stellen Sie außerdem sicher, dass die IBM Business Monitor-Datenbank auf dem fernen IBM Cognos BI-Server mit demselben Namen wie im Katalogeintrag auf dem IBM Business Monitor-Server katalogisiert wurde.

Wenn Sie über die Administrationskonsole eine Implementierungsumgebung erstellt haben, dann wurde eine neue IBM Cognos BI-Installation für Sie erstellt. Um sie zu entfernen, müssen Sie den Befehl **wbmRemoveCognosService** verwenden. (Wenn Sie vor der Erstellung einer Implementierungsumgebung den Befehl **wbmSetCognosDispatcher** ausgeführt haben, wurde der IBM Cognos BI-Service nicht implementiert und muss daher nicht entfernt werden.)

Um Business Space so einzurichten, dass das Produkt mit einem vorhandenen IBM Cognos BI-System arbeiten kann, müssen Sie die folgenden Schritte ausführen:

1. Konfigurieren Sie Single Sign-on zwischen dem WebSphere Application Server-System, auf dem Business Space ausgeführt wird, und dem WebSphere Application Server-System, auf dem IBM Cognos BI ausgeführt wird. Weitere Informationen hierzu finden Sie im Abschnitt Single Sign-on aktivieren.
2. Konfigurieren Sie IBM Cognos BI für Single Sign-on. Weitere Informationen hierzu finden Sie im Abschnitt Vorhandenen IBM Cognos BI-Service für Single Sign-on konfigurieren.
3. Fügen Sie den Hostnamen und die Portnummer für IBM Cognos BI der Liste der vertrauenswürdigen Server in IBM Cognos BI hinzu. Andernfalls können Sie die Seiten in Business Space nicht anzeigen.
  - a. Öffnen Sie den IBM Cognos BI-Konfigurationsclient. Führen Sie zum Öffnen des Clients die Datei `cogconfig.bat` oder `cogconfig.sh` aus, die sich für 32-Bit-Server in `cognos-installationsstammverzeichnis/bin` oder für 64-Bit-Server in `cognos-installationsstammverzeichnis/bin64` befindet.
  - b. Wählen Sie **Lokale Konfiguration > Sicherheit > IBM Cognos Application Firewall** aus.
  - c. Klicken Sie auf das Stiftsymbol neben **Gültige Domänen oder Hosts** und fügen Sie den IBM Cognos BI-Host und die Portnummer hinzu, die im Endpunkt von Business Space konfiguriert sind. Fügen Sie beispielsweise `1c2d266009.example.com:9080` hinzu. Wenn Sie über mehrere Hosts verfügen, klicken Sie auf **Hinzufügen**, um weitere Einträge hinzuzufügen.
  - d. Klicken Sie auf **OK**. Klicken Sie auf **Speichern**.
  - e. Starten Sie den Server, der IBM Cognos BI ausführt, erneut.

4. Da Business Space-Endpunkte für IBM Cognos BI konfiguriert werden, wenn die ferne URL für IBM Cognos BI konfiguriert wird, überprüfen Sie, ob die angepassten Eigenschaften des Ressourcenumgebungsproviders Mashups Endpoints korrekt sind:

- a. Klicken Sie in der WebSphere-Administrationskonsole auf **Ressourcen**.
- b. Überprüfen Sie die folgenden angepassten Eigenschaften für den Ressourcenumgebungsprovider Mashups Endpoints:

```
{com.ibm.cognos}cognosServiceRootId.url
{com.ibm.cognos}cognosDispatcherRootId.url
{com.ibm.cognos}cognosWebContentRootId.url
```

5. Wenn die Eigenschaften, die Sie in Schritt 4 überprüft haben, nicht korrekt sind, führen Sie die folgenden Schritte aus:

- a. Aktualisieren Sie die folgende Serviceendpunktdatei:

*installationsverzeichnis/BusinessSpace/registryData/WBM/endpoints/cognosEndpoints.xml* Fügen Sie in jedem der drei `<tns:url>`-Abschnitte den Hostnamen für den IBM Cognos BI-Server und den Port am Zeilenanfang ein.

Wenn der Hostname zum Beispiel `1c2d266009.example.com` lautet und Ihr Port `9080` heißt, müsste die entsprechend vervollständigte Datei wie folgt aussehen:

```
<tns:Endpoint>
<tns:id>{com.ibm.cognos}cognosServiceRootId</tns:id>
<tns:type>{com.ibm.cognos}cognosServiceRootId</tns:type>
<tns:version>1.0.0.0</tns:version>
<tns:url>http://1c2d266009.example.com:9080/p2pd/servlet/dispatch/ext/</tns:url>
<tns:description>Position von Sicherungsservices für Cognos-Widgets</tns:description>
</tns:Endpoint>
```

```
<tns:Endpoint>
<tns:id>{com.ibm.cognos}cognosDispatcherRootId</tns:id>
<tns:type>{com.ibm.cognos}cognosDispatcherRootId</tns:type>
<tns:version>1.0.0.0</tns:version>
<tns:url>http://1c2d266009.example.com:9080/p2pd/servlet/dispatch/ext/</tns:url>
<tns:description>Position von Cognos Dispatcher</tns:description>
</tns:Endpoint>
```

```
<tns:Endpoint>
<tns:id>{com.ibm.cognos}cognosWebContentRootId</tns:id>
<tns:type>{com.ibm.cognos}cognosWebContentRootId</tns:type>
<tns:version>1.0.0.0</tns:version>
<tns:url>http://1c2d266009.example.com:9080/p2pd/servlet/</tns:url>
<tns:description>Position von Cognos-Webinhalt</tns:description>
</tns:Endpoint>
</tns:BusinessSpaceRegistry>
```

Weitere Informationen zum Ändern der Endpunktdateien finden Sie im Abschnitt zum Aktivieren von Business Space-Widgets für zellenübergreifende Umgebungen.







- b. Führen Sie den Befehl **updateBusinessSpaceWidgets** für die Datei `cognosEndpoints.xml` aus. Führen Sie die Anweisungen im Abschnitt zum Aktivieren von Business Space-Widgets für zellenübergreifende Umgebungen aus.

## IBM Cognos BI mit WebSphere Portal konfigurieren


Wenn Sie IBM Cognos Business Intelligence zusammen mit WebSphere Portal verwenden, müssen Sie den Abschnitt `ProxyServlet_Servlet` in der Datei `web.xml` aktualisieren.





Vollständige Informationen zum Konfigurieren von Business Space zur Verwendung mit WebSphere Portal finden Sie im Abschnitt "Widgets zur Verwendung mit WebSphere Portal konfigurieren"

1. Exportieren Sie die EAR-Datei (EAR = Enterprise Archive) von WebSphere Portal mit dem Namen `wps.ear` entsprechend Ihrer Netzkonfiguration. Wenn Sie über eine Clusterumgebung verfügen, muss die EAR-Datei von WebSphere Portal von der Network Deployment-Maschine von WebSphere Application Server exportiert werden.
  - a. Wechseln Sie in der Befehlszeile ins Verzeichnis `profilstammverzeichnis_anwendungsserver/bin`.
  - b. Führen Sie den folgenden Befehl aus, um die Datei `wps.ear` in ein temporäres Verzeichnis zu exportieren und vergewissern Sie sich dabei, dass alle Befehle in einer Zeile eingegeben werden:
    -  `wsadmin.bat -user admin_benutzer_id -password admin_kennwort -c "$AdminApp export wps verzeichnis/wps.ear"`
    -   `./wsadmin.sh -user admin_benutzer_id -password admin_kennwort -c '$AdminApp export wps verzeichnis/wps.ear'`Dabei ist `admin_benutzer_id` die Benutzer-ID des Administrators, `admin_kennwort` sein Kennwort und `verzeichnis` das temporäre Verzeichnis.
2. Erstellen Sie das Unterverzeichnis `/wps_expanded`. Verwenden Sie das Scripting-Tool **EARExpander**, um die Inhalte der exportierten EAR-Datei zu erweitern. (Vergewissern Sie sich dabei, dass alle Befehle in einer Zeile eingegeben werden.)
  -  `EARExpander.bat -ear verzeichnis\wps.ear -operationDir verzeichnis\wps_expanded -operation expand`
  -   `./EARExpander.sh -ear verzeichnis/wps.ear -operationDir verzeichnis/wps_expanded -operation expand`
3. Erstellen Sie eine Sicherungskopie von `verzeichnis/wps_expanded/wps.war/WEB-INF/web.xml`.
4. Aktualisieren Sie `verzeichnis/wps_expanded/wps.war/WEB-INF/web.xml`.
  - a. Öffnen Sie die Datei `web.xml`.
  - b. Suchen Sie den folgenden Abschnitt:




```
<servlet id="ProxyServlet_Servlet">
  <servlet-name>ProxyServlet</servlet-name>
  <servlet-class>com.ibm.wps.proxy.servlet.ProxyServlet</servlet-class>
</servlet>
```
  - c. Ersetzen Sie den Abschnitt durch folgenden Text:

```
<servlet id="ProxyServlet_Servlet">
  <servlet-name>ProxyServlet</servlet-name>
  <servlet-class>com.ibm.wps.proxy.servlet.ProxyServlet</servlet-class>
  <init-param>
    <param-name>useCtxPathForCookies</param-name>
    <param-value>true</param-value>
  </init-param>
</servlet>
```
5. Löschen Sie die ursprüngliche Datei `wps.ear` aus dem Verzeichnis, in das Sie sie ursprünglich exportiert haben.
6. Verwenden Sie den Befehl **EARExpander**, um das Verzeichnis der EAR-Datei wieder in einer EAR-Datei zu komprimieren.
  -  `EARExpander.bat -ear verzeichnis\wps.ear -operationDir verzeichnis\wps_expanded -operation collapse`



-   `./EARExpander.sh -ear directory/wps.ear -operationDir verzeichnis/wps_expanded -operation collapse`
7. Verwenden Sie den Befehl 'wsadmin', um die EAR-Datei von WebSphere Portal zu aktualisieren.

**Anmerkung:** Wenn es sich hier um eine verwaltete Zelle (mit oder ohne Cluster) handelt, für Sie diesen Schritt auf der Deployment Manager-Maschine aus.

-  `wsadmin.bat -user admin_benutzer_id -password admin_kennwort -c "$AdminApp install verzeichnis/wps.ear {-update -appname wps -nodeployejb}"`
-   `./wsadmin.sh -user admin_benutzer_id -password admin_kennwort -c '$AdminApp install verzeichnis/wps.ear {-update -appname wps -nodeployejb}'`

Dabei ist *admin\_benutzer\_id* die Benutzer-ID des Administrators, *admin\_kennwort* sein Kennwort und *verzeichnis* das temporäre Verzeichnis.

8. Starten Sie den WebSphere Portal-Server erneut. In einer Clusterkonfiguration müssen Sie für den Cluster einen Neustart durchführen.
9. Fügen Sie den Hostnamen und die Portnummer für IBM Cognos BI der Liste der vertrauenswürdigen Server in IBM Cognos BI hinzu. Andernfalls können Sie die Seiten in Business Space nicht anzeigen.
- Öffnen Sie den IBM Cognos BI-Konfigurationsclient. Führen Sie zum Öffnen des Clients die Datei cogconfig.bat oder cogconfig.sh aus, die sich für 32-Bit-Server in *cognos-installationsstammverzeichnis*/bin oder für 64-Bit-Server in *cognos-installationsstammverzeichnis*/bin64 befindet.
  - Wählen Sie **Lokale Konfiguration > Sicherheit > IBM Cognos Application Firewall** aus.
  - Klicken Sie auf das Stiftsymbol neben **Gültige Domänen oder Hosts** und fügen Sie den IBM Cognos BI-Host und die Portnummer hinzu, die im Endpunkt von Business Space konfiguriert sind. Fügen Sie beispielsweise `1c2d266009.example.com:9080` hinzu. Wenn Sie über mehrere Hosts verfügen, klicken Sie auf **Hinzufügen**, um weitere Einträge hinzuzufügen.
  - Klicken Sie auf **OK**. Klicken Sie auf **Speichern**.
  - Starten Sie den Server, der IBM Cognos BI ausführt, erneut.

## Berichtsdatenquelle in IBM Cognos BI konfigurieren

Wenn Sie Würfelpakete für Ihr erstes Monitormodell veröffentlichen, wird eine Berichtsdatenquelle mit dem Namen WBMONITOR\_DB automatisch in IBM Cognos BI erstellt. Die Datenquelle WBMONITOR\_DB wird verwendet, um für die dimensionale Berichterstellung eine Verbindung zu der MONITOR-Datenbank herzustellen.

Die Datenquelle WBMONITOR\_DB wird auf der Basis der Werte konfiguriert, die aus der WebSphere Application Server-JDBC-Datenquelle mit dem Namen `monitor_database` kopiert wurden.

Wenn Sie Würfelpakete aufgrund von Problemen mit der Datenbankverbindung nicht veröffentlichen können oder wenn Sie den Benutzernamen oder das Kennwort für die IBM Business Monitor-Datenbank ändern, müssen Sie die Verbindung zu der Datenquelle WBMONITOR\_DB mit dem IBM Cognos-Verwaltungsclient rekonfigurieren. Alternativ können Sie die Datenquelle WBMONITOR\_DB im IBM Cognos-Verwaltungsclient löschen und ein Würfelpaket mithilfe der Seite 'Cognos-Würfel verwalten' der IBM Business Monitor-Administrationskonsole erneut veröf-

fentlichen. Daraufhin wird die Datenquelle WBMONITOR\_DB auf der Basis der neuesten Konfigurationswerte in der WebSphere Application Server-JDBC-Datenquelle mit dem Namen Monitor\_database automatisch neu generiert.

1. Starten Sie den IBM Cognos-Verwaltungsclient unter `http://hostname:portnummer/p2pd/servlet/dispatch/ext`.
2. Rufen Sie **IBM Cognos Administration > Konfiguration > Datenquellenverbindungen > WBMONITOR\_DB** auf. Von dieser Seite aus können Sie die Verbindung konfigurieren und testen sowie den Benutzernamen und das Kennwort bearbeiten.

**Tipp:** Wenn Sie die Verbindung zu WBMONITOR\_DB testen, sollten zwei Nachrichten mit dem Wort **Erfolgreich** angezeigt werden.

- Die erste Nachricht weist den Typ "IBM DB2 / Kompatibel" (oder "Oracle / Kompatibel" oder "SQL Server / Kompatibel") auf. Diese Nachricht betrifft die Verbindung, die den nativen Datenbankclient verwendet und zum Veröffentlichlichen von Würfelpaketen erforderlich ist.
- Die zweite Nachricht weist den Typ " / Dynamisch" auf. Diese Nachricht betrifft die JDBC-Verbindung des Typs 4, die zum Ausführen von IBM Cognos BI-Berichten erforderlich ist.

Wird bei einem dieser Verbindungstypen **Fehlgeschlagen** angezeigt, bearbeiten Sie die entsprechenden Konfigurations- oder Anmeldeinformationen und testen Sie die Verbindung erneut. Wenn andere Verbindungstypen fehlschlagen, können Sie dies ignorieren.

---

## IBM Business Monitor-Widgets für WebSphere Portal konfigurieren

IBM Business Monitor stellt keine portletbasierten Dashboards mehr zur Verfügung. Allerdings können Ihre IBM Business Monitor-Widgets in WebSphere Portal weiterhin angezeigt werden.

Führen Sie die folgenden allgemeinen Schritte aus, um Widgets in WebSphere Portal anzuzeigen:

1. Business Space konfigurieren.
2. Widgets zur Verwendung mit WebSphere Portal konfigurieren.
3. IBM Cognos Business Intelligence zur Verwendung mit WebSphere Portal konfigurieren.

---

## Empfang von Ereignissen konfigurieren

Sie können konfigurieren, wie Ereignisse von Anwendungen an die CEI (Common Event Infrastructure) fließen und wie sie von der CEI an IBM Business Monitor fließen.

### Hinweise zu asynchronen Ereignissen

Der Datenfluss von einer ausgebenden Anwendung zur CEI (Common Event Infrastructure) kann synchron oder asynchron erfolgen. Bei der synchronen Ereignisübertragung wartet eine Anwendung auf die erfolgreiche Ereigniszustellung, bevor sie den Rest der Transaktion fortsetzt. Bei der asynchronen Ereignisübertragung stellt eine Anwendung Ereignisse in eine Warteschlange und fährt mit der Verarbeitung fort.

Wenn Sie die asynchrone Ereignisübertragung verwenden, können Sie die Auswirkungen auf die ausgebende Anwendung minimieren, was bei der Überwachung

von unternehmenskritischen Anwendungen von großer Bedeutung sein kann. Jedoch können bei der asynchronen Ereignisübertragung Ereignisse von einem Monitormodell in einer anderen Reihenfolge empfangen werden, als sie in der ausgehenden Anwendung aufgetreten sind.

Bei Modellen, in denen die Ereignisfolge wichtig ist, kann eine falsche Ereignissequenz zu Ausnahmebedingungen bei der Modellverarbeitung und falsch berechneten Daten führen. Wenn Sie eine feste Ereignisfolge benötigen, müssen Sie sicherstellen, dass die Anwendung, die Ereignisse an IBM Business Monitor ausgibt, mit der synchronen Ereignisausgabe arbeitet. Sie können auch im Monitormodell einen Ereignissequenzpfad definieren, um die Reihenfolge der Ereignisverarbeitung festzulegen.

In der Administrationskonsole unter **Serviceintegration > Common Event Infrastructure > Ereignis-Emitter-Factories** können Sie zum Beispiel überprüfen, ob die Ereignisausgabe asynchron erfolgt. Wählen Sie die Emitter-Factory aus, die einen Namen wie **Standard-CEI-Emitter** haben kann. Die Anzeige, die daraufhin geöffnet wird, enthält einen Bereich für die Ereignisübertragung mit Einstellungen zur Steuerung der Ereignisausgabe. Die JMS-Übertragung erfolgt asynchron und die Ereignisserviceübertragung erfolgt synchron.

Wenn Sie mit der asynchronen Ereignisübertragung arbeiten möchten und die Ereignisse in der Reihenfolge ihrer Erstellung verarbeitet verwenden sollen, müssen Sie im Monitormodell einen Ereignissequenzpfad definieren. Weitere Informationen zum Definieren von Ereignissequenzpfaden erhalten Sie über die zugehörigen Links.

### **Autorisierung für asynchrone Ereigniszustellung konfigurieren**

Wenn Sie planen, Ereignisse zu empfangen, die von einer Anwendung ausgegeben werden, welche eine Ereignis-Emitter-Factory mit asynchroner Übermittlung verwendet, und Sie Ihre Umgebung nicht mithilfe des Konfigurationsassistenten der Implementierungsumgebung oder von `wbmDeployCEIEventService AdminTask` eingerichtet haben, müssen Sie den IBM Business Monitor-Server für die Kommunikation mit dem CEI-Server (CEI = Common Event Infrastructure) konfigurieren.

Wenn Sie Ihre Umgebung mithilfe des Konfigurationsassistenten der Implementierungsumgebung oder von `wbmDeployCEIEventService AdminTask` eingerichtet haben, wird diese Konfiguration für Sie durchgeführt. Sie müssen diese Task zum Konfigurieren der Berechtigungsinformationen für JMS nur ausführen, wenn Sie einen eigenen CEI-Server konfigurieren oder eine nicht der Standardeinheit entsprechende Ereignis-Emitter-Factory und nicht den Common Event Infrastructure-Standardemitter verwenden.

Bevor Sie mit dieser Task beginnen, müssen Sie sich bei der Administrationskonsole von WebSphere Application Server anmelden. Wenn Sie einen fernen CEI-Server und die warteschlangenbasierte Methode zum Empfang von Ereignissen verwenden, müssen Sie die Service Integration Bus-Links konfigurieren, bevor Sie mit dieser Task beginnen. Weitere Informationen finden Sie in der verwandten Task 'Warteschlangenbasiertes Ereignismanagement in einer Mehrzellenumgebung konfigurieren'.

Alternativ zur Verwendung der Administrationskonsole können Sie die `wsadmin-Task setEventServiceJmsAuthAlias` ausführen, um die Schritte durchzuführen, die in diesem Abschnitt beschrieben werden.

Führen Sie in der Administrationskonsole von WebSphere Application Server die folgenden Schritte aus:

1. Geben Sie die Autorisierungsaliasnamen für die Warteschlangenverbindungsfactory an.
  - a. Klicken Sie in der Navigationsanzeige auf **Ressourcen > JMS > Warteschlangenverbindungsfactorys**.
  - b. Klicken Sie in der Liste der Warteschlangenverbindungsfactorys auf **CommonEventInfrastructure\_QueueCF**.
  - c. Wählen Sie im Abschnitt mit den Sicherheitseinstellungen einen Aliasnamen aus der Liste **Authentifizierungsalias für die XA-Wiederherstellung** aus. Der Aliasname muss über einen Benutzer mit der Rolle 'Bus-Connector' für den CEI-Bus verfügen. (Klicken Sie unter **Serviceintegration > Busse** auf die Spalte **Sicherheit** für den Bus, der in **CommonEventInfrastructure Bus** beschrieben ist.)
  - d. Wählen Sie einen Aliasnamen aus der Liste **Containergesteuerter Authentifizierungsalias** aus. Normalerweise können Sie denselben Aliasnamen wie im vorherigen Schritt auswählen.
  - e. Klicken Sie auf **OK** und speichern Sie Ihre Änderungen in der Masterkonfiguration.
2. Geben Sie einen Authentifizierungsaliasnamen für die Aktivierungsspezifikation an.
  - a. Klicken Sie in der Navigationsanzeige auf **Ressourcen > JMS > Aktivierungsspezifikationen**.
  - b. Klicken Sie in der Liste der Aktivierungsspezifikationen auf **CommonEventInfrastructure\_ActivationSpec**.
  - c. Wählen Sie im Abschnitt mit den Sicherheitseinstellungen einen Aliasnamen aus der Liste **Authentifizierungsalias** aus.
  - d. Klicken Sie auf **OK** und speichern Sie Ihre Änderungen in der Masterkonfiguration.
3. Geben Sie einen Autorisierungsaliasnamen für die Abschnittsverbindungsfactory an.
  - a. Klicken Sie in der Navigationsanzeige auf **Ressourcen > JMS > Abschnittsverbindungsfactorys**.
  - b. Klicken Sie in der Liste der Abschnittsverbindungsfactorys auf **CommonEventInfrastructure\_AllEventsTopicCF**.
  - c. Wählen Sie im Abschnitt mit den Sicherheitseinstellungen einen Aliasnamen aus der Liste **Authentifizierungsalias für die XA-Wiederherstellung** aus. Der Aliasname muss über einen Benutzer mit der Rolle 'Bus-Connector' für den CEI-Bus verfügen. (Klicken Sie unter **Serviceintegration > Busse** auf die Spalte **Sicherheit** für den Bus, der in **CommonEventInfrastructure Bus** beschrieben ist.)
  - d. Wählen Sie einen Aliasnamen aus der Liste **Containergesteuerter Authentifizierungsalias** aus. Normalerweise können Sie denselben Aliasnamen wie im vorherigen Schritt auswählen.
  - e. Klicken Sie auf **OK** und speichern Sie Ihre Änderungen in der Masterkonfiguration.

## Ereignisse von der CEI empfangen

In IBM Business Monitor können Sie angeben, dass Ereignisse vom CEI-Server (CEI = Common Event Infrastructure) für eingehende Nachrichten anhand von

zwei unterschiedlichen Übertragungstypen empfangen werden sollen: JMS-Methode (warteschlangenbasiert) oder tabellenbasierte Methode (auch als Warteschlangenumgehung bezeichnet).

Die warteschlangenbasierte Ereigniszustellung verwendet JMS (Java Messaging Service), um Ereignisse von CEI zum Monitormodell zu übertragen. Tabellenbasierte Ereigniszustellung (bisher unter der Bezeichnung "Warteschlangenumgehung") verwendet eine Datenbanktabelle, um Ereignisse von CEI zum Monitormodell zu übertragen.

Bei der tabellenbasierten Ereigniszustellung kann die Arbeit unter mehreren Cluster-Mitgliedern aufgeteilt werden. Darüber hinaus übergeht Ereignisdatenfluss die JMS-Warteschlange des Monitor-Modells leitet alle Ereignisse direkt an die Ereignisdatenbanktabelle des Modells. In den meisten Umgebungen verbessert diese Methode die Leistung, da ein für die JMS-Warteschlange erforderlicher Persistenzschritt entfällt. Weitere Vorteile der tabellenbasierten Methode bestehen darin, dass Sie weder den Service Integration Bus noch den zugehörigen Link für den Empfang von Ereignissen aus einer fernen Zelle konfigurieren müssen und Modelle aus früheren Versionen erneut erstellen können, sodass diese diese Methode verwenden.

### **Ereignisse mithilfe der tabellenbasierten Ereigniszustellung empfangen**

Sie können Ihren CEI-Ereignisservice (CEI = Common Event Infrastructure) so konfigurieren, dass die Ereignisse an die Ereignisdatenbanktabelle für das Monitormodell gesendet werden. Sie müssen den Service Integration Bus-Link und die zugehörigen Ressourcen nicht konfigurieren. Durch die Umgehung der JMS-Warteschlange wird die Leistung verbessert, da ein zusätzlicher Datenspeicherungsschritt entfällt, der bei Verwendung der Warteschlange erforderlich ist.

Beim Einsatz der tabellenbasierten Ereigniszustellung in IBM Business Monitor 7.5 kann die Arbeit unter mehreren Cluster-Mitgliedern aufgeteilt werden. In den meisten Umgebungen verbessert diese Methode die Leistung und vereinfacht die Systemkonfiguration.

- **Modelle vor Version 6.2:** Tabellenbasierte Ereigniszustellung wird nicht unterstützt. Um diese Methode für Monitormodelle aus einer Version vor Version 6.2 verwenden zu können, müssen Sie mit dem Business Monitor Development Toolkit zuerst ein Upgrade des Monitormodells durchführen. Ändern Sie die Versionsnummer, generieren Sie eine neue EAR-Datei und implementieren Sie eine neue Version des Monitormodells. Wenn Sie das Upgrade des Modells nicht durchführen möchten, müssen Sie die warteschlangenbasierte Ereigniszustellung verwenden.
- **Modelle der Version 6.2 und 7:** Diese Modelle sind in der Lage, tabellenbasierte Ereigniszustellungen zu verwenden (bisher unter der Bezeichnung Warteschlangenumgehung bekannt). Wenn Sie die verbesserte Skalierbarkeit von Version 7.5 nutzen wollen, müssen Sie Ihr Monitormodell mithilfe eines Business Monitor Development Toolkit, Version 7.5, aufrüsten.
- **Modelle der Version 7.5:** Diese Modelle profitieren bereits von den verbesserten Möglichkeiten der Skalierbarkeit, wenn Sie die tabellenbasierte Ereigniszustellung einsetzen.

**Einschränkung:** Wenn Sie als Datenbank SQL Server verwenden, können Sie die tabellenbasierte Methode der Ereigniszustellung nicht verwenden, es sei denn, die

ausgebende Anwendung wird unter WebSphere Application Server ab Version 7.0 (oder Process Server ab Version 7.0) ausgeführt. Sie müssen die warteschlangenbasierte Methode verwenden.

Sie können die tabellenbasierte Methode in einer Einzelzellen- oder Mehrzellenumgebung aktivieren. Wählen Sie abhängig von Ihrer Umgebung folgende Task aus, um die Konfiguration für diese Methode abzuschließen.

#### **Tabellenbasierte Ereigniszustellung in einer Einzelzellenumgebung konfigurieren:**

Wenn Sie über eine (eigenständige) Einzelserverumgebung verfügen oder wenn auf Ihrem System IBM Business Monitor ab Version 7.0 (oder Version 7.0.0.3 für z/OS) auf allen Knoten der Zelle installiert ist, dann sind zum Empfangen von Ereignissen keine weiteren Schritte erforderlich. Wenn der CEI-Ereignisservice (CEI = Common Event Infrastructure) ohne IBM Business Monitor oder Process Server auf einem Knoten implementiert ist, müssen die IBM Business Monitor-JAR-Dateien für das Routing der Ereignisse auf diesem CEI-Knoten installiert werden.

Process Server ab Version 7.0 auf verteilten Plattformen (und Process Server ab Version 7.0.0.3 auf z/OS-Plattformen) stellt die Dateien bereit, die erforderlich sind, um die Ausgabe ferner Ereignisse zu unterstützen. Wenn Sie eine frühere Version von Process Server verwenden, führen Sie die folgenden Schritte aus, um die tabellenbasierte Ereigniszustellung in einer Einzelzellenumgebung zu konfigurieren.

1. Suchen Sie die Datei, die Ihrem Betriebssystem und der WebSphere Application Server-Version entspricht, unter der der CEI-Ereignisservice ausgeführt wird, im Verzeichnis `application_server-stammverzeichnis/scripts.wbm/crossCell` der lokalen IBM Business Monitor-Serverinstallation.
  - `monitorCommunicationWithWAS70BasedCells.tar`,  
`monitorCommunicationWithWAS61BasedCells.tar`, oder  
`monitorCommunicationWithWAS60BasedCells.tar`.
  - `monitorCommunicationWithWAS70BasedCells.zip`,  
`monitorCommunicationWithWAS61BasedCells.zip`, oder  
`monitorCommunicationWithWAS60BasedCells.zip`.
2. Kopieren Sie die entsprechende Datei in das Verzeichnis `application_server-stammverzeichnis/plugins` auf allen WebSphere Application Server-Installationen auf dem fernen Knoten, der eine CEI-Zieleinheit betreibt und auf dem IBM Business Monitor oder Process Server ab Version 7.0 (oder Version 7.0.0.3 für z/OS) nicht installiert ist, und extrahieren Sie den Inhalt.
3. Führen Sie in jeder WebSphere Application Server-Installation, in die Sie den Inhalt der Datei extrahiert haben, folgende Tasks aus:
  - a. Schalten Sie alle Java Virtual Machines (JVMs) ab, die `application_server-stammverzeichnis/java/bin/java` verwenden, einschließlich Knotenagenten, Server, Deployment Manager und `wsadmin`-Eingabeaufforderungen.
  - b. Führen Sie `profil-stammverzeichnis/bin/osgiCfgInit` für jedes Profil in der WebSphere Application Server-Installation aus.
  - c. Führen Sie für alle Knotenagenten und Server einen Neustart durch.

#### **Tabellenbasierte Ereigniszustellung in einer Mehrzellenumgebung konfigurieren:**

Wenn Ihr IBM Business Monitor in einer anderen Zelle als der CEI-Ereignisservice installiert ist, ist die Durchführung zusätzlicher Konfigurationsschritte erforderlich, um die Kommunikation zwischen den Zellen zu aktivieren.



Bei geschützten Umgebungen sollten Sie sich vor der Ausführung dieser Task zudem vergewissern, dass folgende Tasks ausgeführt wurden:

- Wenn in der fernen oder der lokalen Zelle die Sicherheit aktiviert ist, dann muss diese auch für die jeweils andere Zelle aktiviert werden.
- Wenn die Sicherheit aktiviert ist, müssen Sie die Server-to-Server-Trust-Funktion (SSL) zwischen dem fernen CEI-Server und dem lokalen IBM Business Monitor-Server aktivieren (siehe hierzu den Abschnitt Server-zu-Server-SSL in einer Umgebung mit mehreren Zellen konfigurieren).
- LTPA-Schlüssel müssen von den Zellen gemeinsam genutzt werden und die Zellen müssen dieselbe ID aufweisen (siehe hierzu den Abschnitt LTPA-Schlüssel gemeinsam nutzen).
- Die Einstellung **Identitätszusicherung verwenden** muss in der lokalen und in der fernen Zelle aktiviert sein (siehe hierzu den Abschnitt Identitätszusicherung aktivieren).

Falls IBM Business Monitor in einer Umgebung mit mehreren Zellen nicht in der fernen Zelle installiert ist, die Ereignisse ausgibt, müssen Sie den Deployment Manager und die CEI-Server in der fernen Zelle konfigurieren, damit sie Ereignisse an die Tabellen ausgeben können. Process Server ab Version 7.0 auf verteilten Plattformen (und Process Server ab Version 7.0.0.3 auf z/OS-Plattformen) stellt die Dateien bereit, die erforderlich sind, um die Ausgabe ferner Ereignisse zu unterstützen. Vorherige Versionen von Process Server stellen diese Dateien nicht automatisch zur Verfügung. Daher unterscheiden sich die Anweisungen abhängig davon, ob die ferne Zelle, die Ereignisse ausgibt, eine verteilte Zelle mit einer Installation von Process Server ab Version 7.0 (Version 7.0.0.3 für z/OS) ist.

Um die tabellenbasierte Ereigniszustellung zellenübergreifend zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

- Wenn in der fernen Zelle (Zelle ohne IBM Business Monitor) Process Server ab Version 7.0 (Version 7.0.0.3 für z/OS) **nicht** installiert ist:
  1. Suchen Sie die Datei, die Ihrem Betriebssystem und der WebSphere Application Server-Version entspricht, unter der der CEI-Ereignisservice ausgeführt wird, im Verzeichnis `application_server-stammverzeichnis/scripts.wbm/crossCell` der lokalen IBM Business Monitor-Serverinstallation.
    - `monitorCommunicationWithWAS70BasedCells.tar` oder `monitorCommunicationWithWAS61BasedCells.tar`.
    - `monitorCommunicationWithWAS70BasedCells.zip` oder `monitorCommunicationWithWAS61BasedCells.zip`.
  2. Kopieren Sie die entsprechende Datei in das Verzeichnis `application_server-stammverzeichnis/plugins` des Remote Deployment Managers und extrahieren Sie den Inhalt.
  3. Kopieren Sie dieselbe Datei in das Verzeichnis `application_server-stammverzeichnis/plugins` auf jeder WebSphere Application Server-Installation in der fernen Zelle, die eine CEI-Zieleinheit betreibt und auf der IBM Business Monitor oder Process Server ab Version 7.0 (oder Version 7.0.0.3 für z/OS) nicht installiert ist.
  4. Führen Sie in jeder WebSphere Application Server-Installation, in die Sie den Inhalt der Datei extrahiert haben, folgende Tasks aus:
    - a. Schalten Sie alle Java Virtual Machines (JVMs) ab, die `application_server-stammverzeichnis/java/bin/java` verwenden, einschließlich Knotenagenten, Server, Deployment Manager und `wsadmin`-Eingabeaufforderungen.



- b. Führen Sie `profil-stammverzeichnis/bin/osgiCfgInit` für jedes Profil in der WebSphere Application Server-Installation aus.
  - c. Führen Sie für alle Knotenagenten und Server einen Neustart durch.
5. Führen Sie auf dem Remote Deployment Manager bzw. dem eigenständigen Server den `wsadmin`-Befehl `wbmConfigureQueueBypassDataSource` aus. Ein Beispiel sowie eine Liste der Parameter für diesen Befehl finden Sie im Abschnitt zur tabellenbasierten CEI in mehreren Zellen. Führen Sie nach der Ausführung des Befehls und der Speicherung der Konfigurationsänderungen einen Neustart des Remote Deployment Managers bzw. des eigenständigen Servers durch.
- Wenn in der fernen Zelle Process Server ab Version 7.0 (oder Version 7.0.0.3 für z/OS) installiert ist:
    1. Führen Sie auf dem Remote Deployment Manager bzw. dem eigenständigen Server den `wsadmin`-Befehl `wbmConfigureQueueBypassDataSource` aus. Ein Beispiel sowie eine Liste der Parameter für diesen Befehl finden Sie im Abschnitt zur tabellenbasierten CEI in mehreren Zellen.
    2. Führen Sie nach der Ausführung des Befehls und der Speicherung der Konfigurationsänderungen einen Neustart des Remote Deployment Managers bzw. des eigenständigen Servers durch.

Bei der Implementierung eines Monitormodells mit einer fernen CEI müssen Sie die **Ferne** CEI-Positionsoption auswählen, wie im Schritt "CEI-Optionen für Monitormodell auswählen" im Thema Monitormodelle implementieren beschrieben.

**Wenn Sie einen CEI-Server unter z/OS ausführen:** Nach Abschluss der tabellenbasierten CEI-Konfiguration wird der folgende Fehler in den CEI-Protokollen unter z/OS aufgezeichnet, wenn Sie ein Monitormodell implementieren:

```
CEI61Configur E
com.ibm.wbimonitor.observationmgr.spi.impl.CEI61RemoteConfigurationSessionImpl reloadCEIConfig(Str
```

Führen Sie die folgenden Schritte aus, um die CEI-Konfiguration durchzuführen:

1. Starten Sie den CEI-Server oder -Cluster erneut (für die Ausgabe von CEI unter z/OS).
2. Führen Sie mit dem Deployment Manager von IBM Business Monitor die Methode `confirmCEIServerReboot(String modelID)` der Lifecycle Services-MBean aus, um anzuzeigen, dass die CEI erneut gestartet wurde. Führen Sie folgende Schritte aus, um den Befehl von einer `wsadmin`-Eingabeaufforderung auszuführen:
  - a. Stellen Sie eine Verbindung zur Lifecycle Services-MBean her:
 

```
wsadmin> set ls [$AdminControl completeObjectName type=LifecycleServices,*]
```
  - b. Bestätigen Sie, dass die CEI erneut gestartet wurde:
 

```
wsadmin> $AdminControl invoke $ls confirmCEIServerReboot { "<model ID>" }
```

## Ereignisse mithilfe der warteschlangenbasierten Ereigniszustellung empfangen

Um Ereignisse mit JMS-Warteschlangen (JMS = Java Message Service) zu empfangen, müssen Sie keine zusätzlichen Schritte ausführen, es sei denn, Sie wollen die Kommunikation zwischen dem IBM Business Monitor-Server und einem fernen CEI-Server aktivieren. Wenn Sie ein Monitormodell verwenden, das mithilfe von IBM Business Monitor 6.1 in einer Umgebung mit IBM Business Monitor 8.0 erstellt wurde und für das Monitormodell kein Upgrade ausgeführt wurde, müssen Sie die warteschlangenbasierte Ereignismanagementmethode verwenden.

Sie können warteschlangenbasiertes Ereignismanagement in einer Einzelzellen- oder Mehrzellenumgebung verwenden. Wenn sich Ihr CEI-Server nicht in der Zelle, in der IBM Business Monitor installiert ist, sondern in einer fernen Zelle befindet, ist die Durchführung zusätzlicher Konfigurationsschritte erforderlich, um die Kommunikation zwischen den beiden Zellen zu aktivieren.

#### **Warteschlangenbasierte Ereigniszustellung in einer Einzelzellenumgebung konfigurieren:**

Wenn Ihr IBM Business Monitor in derselben Zelle wie der CEI-Ereigniservice installiert ist und Sie die warteschlangenbasierte Methode zum Empfang von Ereignissen verwenden, müssen keine weiteren Schritte ausgeführt werden. Bei der Installation von IBM Business Monitor wurden die erforderlichen JAR-Dateien in die korrekten Ordner kopiert und der Service Integration Bus erstellt.

#### **Warteschlangenbasierte Ereigniszustellung in einer Mehrzellenumgebung konfigurieren:**

Wenn Ihr IBM Business Monitor in einer anderen Zelle als der CEI-Server installiert ist, ist die Durchführung zusätzlicher Konfigurationsschritte erforderlich, um die Kommunikation zwischen den Zellen zu aktivieren. Um Ereignisse aus der JMS-Warteschlange in dieser zellenübergreifenden Umgebung empfangen zu können, muss der IBM Business Monitor-Server für den Empfang von CEI-Ereignissen (CEI, Common Event Infrastructure) von einem fernen CEI-Server konfiguriert werden.

Vor der Ausführung dieser Task sollten Sie sicherstellen, dass die folgenden Arbeitsschritte bereits ausgeführt wurden:

- Der ferne CEI-Service wurde implementiert und konfiguriert.
- Der Service Integration Bus für den lokalen IBM Business Monitor Server wurde erstellt.

Bei geschützten Umgebungen sollten Sie sich zudem vergewissern, dass folgende Tasks ausgeführt wurden:

- Wenn in der fernen oder der lokalen Zelle die Sicherheit aktiviert ist, dann muss diese auch für die jeweils andere Zelle aktiviert werden.
- Wenn die Sicherheit aktiviert ist, müssen Sie die Server-to-Server-Trust-Funktion (SSL) zwischen dem fernen CEI-Server und dem lokalen IBM Business Monitor-Server aktivieren (siehe hierzu den Abschnitt Server-zu-Server-SSL in einer Umgebung mit mehreren Zellen konfigurieren).
- LTPA-Schlüssel müssen von den Zellen gemeinsam genutzt werden und die Zellen müssen dieselbe ID aufweisen (siehe hierzu den Abschnitt LTPA-Schlüssel gemeinsam nutzen).
- Die Einstellung **Identitätszusicherung verwenden** muss in der lokalen und in der fernen Zelle aktiviert sein (siehe hierzu den Abschnitt Identitätszusicherung aktivieren).

Um die warteschlangenbasierte Ereignismanagementmethode zu konfigurieren, müssen Sie die zellenübergreifenden Dateien installieren, den fernen Service Integration Bus erstellen und den Link zwischen dem lokalen und dem fernen Bus herstellen. Process Server ab Version 7.0 auf verteilten Plattformen (und Process Server ab Version 7.0.0.3 auf z/OS-Plattformen) stellt die Dateien bereit, die erforderlich sind, um die Ausgabe ferner Ereignisse zu unterstützen.

Um das warteschlangenbasierte Ereignismanagement zellenübergreifend zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

**Wichtig:** Wenn Process Server ab Version 7.0 (oder Version 7.0.0.3 für z/OS) in der fernen Zelle installiert ist, können Sie die Schritte 1 - 3 überspringen und direkt mit Schritt 4 fortfahren.

1. Suchen Sie die Datei, die Ihrem Betriebssystem und der WebSphere Application Server-Version entspricht, unter der der CEI-Server ausgeführt wird, im Verzeichnis `application_server-stammverzeichnis/scripts.wbm/crossCell` der lokalen IBM Business Monitor-Serverinstallation.

```
monitorCommunicationWithWAS70BasedCells.tar,  
monitorCommunicationWithWAS61BasedCells.tar, oder  
monitorCommunicationWithWAS60BasedCells.tar.  
  
monitorCommunicationWithWAS70BasedCells.zip,  
monitorCommunicationWithWAS61BasedCells.zip, oder  
monitorCommunicationWithWAS60BasedCells.zip.
```

2. Kopieren Sie die entsprechende Datei in das Verzeichnis `application_server-stammverzeichnis/plugins` des fernen CEI-Servers (eigenständiger Server oder Remote Deployment Manager) und extrahieren Sie den Inhalt.
3. Führen Sie im Verzeichnis `application_server-stammverzeichnis/bin` des fernen CEI-Servers den entsprechenden Befehl aus, um den Anwendungsserver oder Prozessserver so zu konfigurieren, dass dieser die JAR-Datei erkennt: `osgiCfgInit.bat` oder `osgiCfgInit.sh`.
4. Wählen Sie im Verzeichnis `application_server-stammverzeichnis/scripts.wbm/crossCell` der lokalen IBM Business Monitor-Serverinstallation eine der folgenden Methoden aus, um das SIB-Dienstprogramm (SIB = Service Integration Bus) für die zellenübergreifende Konfiguration auszuführen. Weitere Informationen zu diesem Dienstprogramm erhalten Sie über die zugehörigen Links.

- Geben Sie Folgendes ein, um den Befehl interaktiv auszuführen:

```
configRemoteMonitorBus.sh  
configRemoteMonitorBus.bat
```

- Wenn Sie den Befehl anhand einer Eigenschaftendatei ausführen wollen, dann überprüfen Sie die Datei `configRemoteMonitorBus.props` und führen Sie alle notwendigen Änderungen an den Eigenschaften durch. Die Datei `configRemoteMonitorBus.props` stellt eine Beispieleigenschaftendatei dar, die sich im Verzeichnis `application_server-stammverzeichnis/scripts.wbm/crossCell` befindet. Sie können jedoch auch eine eigene Eigenschaftendatei für Ihre Konfiguration erstellen:

```
configRemoteMonitorBus.sh -props eigenschaftendateiname  
configRemoteMonitorBus.bat -props eigenschaftendateiname
```

Dabei gilt Folgendes:

*eigenschaftendateiname* ist der vollständig qualifizierte Name der Eigenschaftendatei, die die erforderlichen Werte für die Konfiguration enthält. Der Pfad der Eigenschaftendatei muss vollständig angegeben sein, damit die Eigenschaftendatei durch das Script gefunden werden kann. Das zellenübergreifende Konfigurationsdienstprogramm erstellt einen Service Integration Bus in der fernen Zelle. Der Name des Busses lautet `MONITOR.<name_der_fernen_zelle>.bus`, wobei `<name_der_fernen_zelle>` für den Namen der fernen Zelle steht.

5. Nach Abschluss des Scripts müssen Sie einen Neustart des lokalen IBM Business Monitor Servers und des fernen CEI-Servers durchführen.

6. Überprüfen Sie, ob der ferne Service Integration Bus vorhanden ist und ob der Link zwischen dem lokalen und dem fernen Bus erfolgreich erstellt werden konnte, indem Sie die Schritte im Abschnitt "Fernen Bus für IBM Business Monitor und Service Integration Link überprüfen" ausführen.

Bei der Implementierung eines Monitormodells mit einer fernen CEI müssen Sie die **Ferne** CEI-Positionsoption auswählen, wie im Schritt "CEI-Optionen für Monitormodell auswählen" im Thema Monitormodelle implementieren beschrieben.

**Bei einer gesicherten Umgebung:** Sie können ein Monitormodell in einer gesicherten Umgebung mit einem fernen CEI und einem warteschlangenbasierten Ereignismanagement implementieren. Nach der Implementierung des Monitormodells müssen Sie die Installation fertigstellen, indem Sie den Anweisungen im Thema "Installation eines Monitormodells in einer geschützten, warteschlangenbasierten Umgebung ausführen" folgen. .

*Fernen Bus für IBM Business Monitor und Service Integration Link überprüfen:*

Nach der Konfiguration des IBM Business Monitor-Servers für die Verwendung des CEI-Servers (CEI = Common Event Infrastructure) auf einem fernen WebSphere Application Server-System oder Process Server-System müssen Sie überprüfen, ob der ferne Bus und der Service Integration Link erfolgreich erstellt wurden.

Um zu überprüfen, ob der ferne Bus und der Service Integration Bus-Link vorhanden und aktiv sind, müssen Sie die folgenden Schritte ausführen:

1. Klicken Sie in der Administrationskonsole auf dem fernen WebSphere Application Server oder Process Server auf **Serviceintegration > Busse**.
2. Klicken Sie auf den Bus MONITOR.<zellenname>.bus, den Sie überprüfen wollen, wobei <zellenname> für den Namen der Zelle steht, in der der ferne CEI-Server installiert ist.
3. Klicken Sie unter 'Topologie' auf **Messaging-Steuerkomponenten**. Eine Messaging-Steuerkomponente ist definiert. Im Feld **Status** wird ein grüner Pfeil angezeigt, wenn die Messaging-Steuerkomponente aktiv ist.
4. Klicken Sie auf die Messaging-Steuerkomponente und dann auf **Weitere Eigenschaften > Service Integration Bus-Links**. Wenn Sie die ferne Zelle mit einer einzelnen Monitor-Installation verbinden und eine Monitor-Installation mit einer einzelnen fernen Zelle, wird nur ein Link definiert. Sie können jedoch auch mehrere Links verwenden. Im Feld **Status** wird ein grüner Pfeil angezeigt, wenn der Link aktiv ist.
5. Optional: Wenn Sie die Überprüfung anhand des Protokolls 'System.out' durchführen wollen, dann suchen Sie nach der folgenden Nachricht. Der Name der Messaging-Steuerkomponente ist auf jedem System unterschiedlich:

CWSIP0382I: Die Messaging-Steuerkomponente FADB84EB685E209F hat auf die Subskriptionsanforderung Die Pub/Sub-Topologie ist jetzt konsistent.

**Anmerkung:** Sie können die gleiche Prozedur auf dem IBM Business Monitor Server ausführen, um festzustellen, ob die Seite des Service Integration Bus-Links für den IBM Business Monitor Server aktiv ist.

---

## Business Space konfigurieren

Sie können Business Space powered by WebSphere konfigurieren. Dieses Produkt stellt eine allgemeine Schnittstelle für Anwendungsbutzer zur Verfügung, über die Sie Webschnittstellen im gesamten Portfolio von IBM Business Process Management, in WebSphere Enterprise Service Bus und in anderen IBM Produkten erstellen, verwalten und integrieren können.

### Business Space konfigurieren

Installieren und konfigurieren Sie Business Space powered by WebSphere, um eine gemeinsame Schnittstelle einzurichten, über die Anwendungsbutzer Webschnittstellen erstellen, verwalten und integrieren können.

Sie müssen die Produktsoftware installieren. Bei der Installation Ihres Produkts werden Business Space-Dateien für die von Ihnen konfigurierten Profile in die Installation eingebunden.

Business Space wird mit folgenden Datenbankprodukten unterstützt:

- DB2 Universal
- DB2 for IBM i
- DB2 for z/OS
- Microsoft SQL Server
- Oracle 11g

Um herauszufinden, welche Datenbanken mit dem IBM Produkt unterstützt werden, das Sie mit Business Space verwenden, ermitteln Sie die für das Produkt unterstützten Datenbanken.

Wenn Sie IBM Business Process Manager, WebSphere Enterprise Service Bus oder IBM Business Monitor installieren und ein eigenständiges Serverprofil mit der Standardoption erstellen, wird Business Space automatisch mit einer DB2 Express-Datenbank installiert und konfiguriert. Wenn Sie ein eigenständiges Serverprofil verwenden, dann können Sie das Profile Management Tool mit der erweiterten Option verwenden, um Business Space für Ihre Laufzeitumgebung zu konfigurieren. Weitere Informationen hierzu finden Sie im Abschnitt "Business Space mit dem Profile Management Tool konfigurieren".

Für alle Produkte gilt: Wenn Sie Deployment Manager- sowie benutzerdefinierte Profile konfigurieren, können Sie die Konfiguration von Business Space am einfachsten mit dem Assistenten für die Konfiguration der Implementierungsumgebung durchführen. Weitere Informationen hierzu finden Sie im Abschnitt "Business Space im Assistenten für die Konfiguration der Implementierungsumgebung konfigurieren".

Wenn Sie eine eigenständige Serverumgebung haben oder die Laufzeitumgebung mit dem Assistenten für die Implementierungsumgebung konfigurieren, werden die REST-Serviceendpunkte automatisch konfiguriert und aktiviert. Konfigurieren Sie die REST-Services in anderen Umgebungen über die Seite der Administrationskonsole für REST-Services. Wenn Widgets in Business Space verfügbar sein sollen, müssen Sie die REST-Serviceendpunkte für diese Widgets konfigurieren. Sie müssen die REST-Endpunkte registrieren, damit Business Space die Widgets den Endpunkten zuordnet und die Widgets in der Palette zur Verwendung angezeigt werden.

Wenn Sie Deployment Manager- und benutzerdefinierte Profile benutzen, können Sie Business Space über die Administrationskonsole konfigurieren.

Wenn die anfängliche Konfiguration im Profile Management Tool oder in der Administrationskonsole funktioniert, müssen Sie außerdem die Datenbanktabellen für Business Space konfigurieren. Weitere Informationen hierzu finden Sie im Abschnitt "Business Space-Datenbanktabellen konfigurieren".

Unabhängig davon, mit welchem Tool Business Space konfiguriert wurde, müssen Sie sicherstellen, dass Business Space in Verbindung mit der Sicherheitsfunktion verwendet werden kann. Weitere Informationen hierzu finden Sie im Abschnitt "Sicherheitsfunktion für Business Space einrichten".

Business Space baut auf der Technologie von IBM Mashup Center auf. Häufig gestellte Fragen und allgemeine Fehlerbehebungsinformationen über IBM Mashup Center finden Sie unter IBM Mashup Center Troubleshooting.

Nachdem Sie Business Space installiert und konfiguriert haben, können die Benutzer Ihrer Laufzeitumgebung das Programm über die folgende URL öffnen: `http://host:port/BusinessSpace`. Hierbei steht *host* für den Namen des Hosts, auf dem Ihr Server ausgeführt wird, und *port* steht für die Portnummer Ihres Servers.

## Business Space mithilfe des Profile Management Tool in einem Produktprofil konfigurieren

Sie können Business Space powered by WebSphere mithilfe des Profile Management Tool in Ihrem Produktprofil konfigurieren.

Sie können das Profile Management Tool nach der Produktinstallation starten. Darüber hinaus können Sie die Funktionalität des Profile Management Tool über die Befehlszeile einsetzen, indem Sie nach der Produktinstallation im Befehlszeilendienstprogramm **manageprofiles** den Parameter **-configureBSpace** verwenden. In beiden Fällen wird Business Space mit demselben Datenbankprodukt installiert, das als Common-Datenbank festgelegt wird. Wenn Sie eine Datenbank ausgewählt haben, die von Business Space nicht unterstützt wird, konfiguriert das Profile Management Tool Business Space mit der IBM DB2 Express-Datenbank.

Ziehen Sie bei Verwendung des Befehlszeilendienstprogramms **manageprofiles** die Dokumentation zu **manageprofiles** für Ihr BPM-Produkt zu Rate. Lesen Sie die folgenden Verwendungshinweise zu **manageprofiles**:

- Wenn Sie Oracle oder SQL Server auf einem eigenständigen Server verwenden, müssen Sie die Datenbank manuell erstellen, anstatt den Parameter **-dbCreateNew** zu verwenden.
- Wenn Sie eine ferne Datenbank in einer Clusterumgebung verwenden, müssen Sie die Datenbank manuell erstellen, die generierten Scripts auf das ferne System mit der Datenbank kopieren und die Scripts auf diesem System ausführen.

Wenn Sie Deployment Manager- oder benutzerdefinierte Profile benutzen, können Sie die Administrationskonsole oder den Assistenten für die Konfiguration der Implementierungsumgebung verwenden. Weitere Informationen zu diesem Thema finden Sie im Abschnitt zur Konfiguration von Business Space über die Administrationskonsole und im Abschnitt zur Konfiguration von Business Space mit dem Assistenten für die Konfiguration der Implementierungsumgebung. Wenn Sie das Profile Management Tool zum Erstellen eines Deployment Managers und benutzerdefinierter Profile (verwaltete Knoten) mit der Profilerstellungsoption **Implementierungsumgebung** verwenden, wird Business Space automatisch mit Ihrer Imple-



mentierungsumgebung konfiguriert, Sie müssen jedoch manuell einige Scripts ausführen, um die Datenbanktabellen zu konfigurieren.

Weiterführende Konfigurationsoptionen für ein eigenständiges Serverprofil sind auf den Seiten der Administrationskonsole für die Konfiguration von Business Space verfügbar. Wenn Sie beispielsweise eine Datenquelle definieren wollen, die von der Datenbank abweicht, die Sie für Ihr Profil ausgewählt haben (die IBM Business Monitor-Datenbank oder die IBM Business Process Manager-Common-Datenbank), müssen Sie zur Konfiguration von Business Space die Administrationskonsole einsetzen.

Wenn Sie diese erweiterten Konfigurationsoptionen einsetzen wollen, die die Verwendung der Administrationskonsole erfordern, dann führen Sie unbedingt die folgenden Arbeitsschritte aus:

- Wenn Sie das eigenständige Serverprofil mithilfe des Profile Management Tool erstellen, dann verwenden Sie die Profilerstellungsoption **Erweitert** und wählen Sie das Kontrollkästchen **Business Space konfigurieren** ab, sodass Sie Business Space zu einem späteren Zeitpunkt über die Administrationskonsole konfigurieren können.
- Weitere Informationen hierzu finden Sie im Abschnitt zum Konfigurieren von Business Space über die Administrationskonsole.

Wenn Sie Business Space nicht in Ihrem Produktprofil konfigurieren möchten, können Sie optional separate Business Space-Profile erstellen. Möglicherweise möchten Sie zur Lastverteilung die Benutzerschnittstelle auf einer Maschine und die Back-End-Verarbeitung auf einer anderen Maschine ausführen. Beispiel: Sie können den IBM Business Process Manager-Server zur Verarbeitung hoher Lasten auf einer Maschine und Business Space auf einer anderen (fernen) Maschine ausführen. Die Back-End-Maschine kann für die Back-End-Verarbeitung optimiert werden und die Business Space-Maschine kann für die Verarbeitung des HTTP-Datenverkehrs eingerichtet werden. Weitere Informationen finden Sie unter „Business Space-Profile erstellen“ auf Seite 190.

- Eigenständiger Server: Starten Sie das Profile Management Tool, wählen Sie die Option **Eigenständiges Serverprofil** aus und führen Sie die folgenden Schritte aus:
  1. Führen Sie auf der Seite mit den Optionen für die Profilerstellung einen der folgenden Schritte aus:
    - Wählen Sie die Option **Typische Profilerstellung** aus, wenn Sie eine Standardinstallation und -konfiguration von Business Space mit der DB2 Express-Datenbank durchführen wollen. (Überspringen Sie die Schritte b bis e.)
    - Wählen Sie die Option **Erweitert** aus, wenn Sie für das Profil, das Sie gerade erstellen, erweiterte Optionen konfigurieren wollen. Stellen Sie sicher, dass auf der Seite 'Business Space - Konfiguration' das Kontrollkästchen **Business Space konfigurieren** ausgewählt ist.

Business Space wird mit der Datenquelle Ihres Produkts konfiguriert.

2. Verwenden Sie bei der Angabe des Hostnamens für Ihr Profil den vollständig qualifizierten Hostnamen.
3. Auf der Seite **Datenbankentwurf** haben Sie die Möglichkeit, eine Datenbankentwurfsdatei zu verwenden, die Sie mit dem Datenbankentwurfstool erstellen und die die gesamte Datenbankkonfiguration für Ihr Produkt enthält, einschließlich der Informationen zur Datenbankkonfiguration für Business



Space. Weitere Informationen zu Datenbankentwurfsdateien finden Sie unter „Eigenschaftendatei für Business Space-Datenbankentwurf erstellen“ auf Seite 254.

4. Führen Sie die Profilerstellung anhand des Profile Management Tools aus. Business Space wird installiert. Das Produkt wird für dasselbe Datenbankprodukt konfiguriert, das Sie als Common-Datenbank festgelegt haben (oder mit DB2 Express, wenn das Datenbankprodukt nicht unterstützt wird).
  5. Wenn sich die Datenbank auf einem fernen System befindet, müssen Sie die Datenbanktabellen konfigurieren, nachdem Sie das Profile Management Tool ausgeführt haben. Weitere Informationen hierzu finden Sie im Abschnitt zur Konfiguration der Business Space-Datenbanktabellen.
- Implementierungsumgebung: Starten Sie das Profile Management Tool, wählen Sie die Option **Deployment Manager-Profil** oder **Benutzerdefiniertes Profil** aus und führen Sie die folgenden Schritte aus.
    1. Wählen Sie auf der Seite mit den Profilerstellungsoptionen die Option **Implementierungsumgebung** aus, um ein Profil mit benutzerdefinierten Konfigurationswerten zu konfigurieren und es in einer Implementierungsumgebung auf der Basis eines bereitgestellten Musters zu verwenden.
    2. Führen Sie mit dem Profile Management Tool die Schritte zum Erstellen eines Deployment Manager-Profiles sowie benutzerdefinierter Profile (verwaltete Knoten) aus.
    3. Nachdem alle benutzerdefinierten Knoten eingebunden sind, führen Sie die entsprechenden Scripts zum Konfigurieren der Datenbanktabellen manuell aus.

**Wichtig:** Wenn Ihre Produktdatenbank eine Oracle-Datenbank ist, wird Business Space mit dem Profile Management Tool oder dem Befehlszeilendienstprogramm manageprofiles so konfiguriert, dass dieselbe Datenbank mit dem Standardschema IBMBUSSP und dem Standardkennwort verwendet wird, das Sie während der Profilerstellung eingegeben hatten. Wenn Sie ein anderes Kennwort für den IBMBUSSP-Benutzernamen festlegen möchten, müssen Sie die Administrationskonsole für die Aktualisierung von JDBC-Ressourcen verwenden:

1. Suchen Sie die Datenquelle jdbc/mashupsDS.
2. Ändern Sie den Wert für den Authentifizierungsalias so, dass er dem Kennwort des Business Space-Schemanamens entspricht.
3. Speichern Sie Ihre Änderungen und starten Sie den Server erneut.

Vor der Verwendung von Business Space müssen Sie die Sicherheitsfunktion einrichten, die für Business Space und die Widgets verwendet werden soll, die von Ihrem Team eingesetzt werden sollen. Weitere Informationen zu diesem Thema finden Sie im Abschnitt zum Einrichten der Sicherheitsfunktion für Business Space.

**Tipp:** Business Space verwendet eine Proxy-Serverkomponente, um eine Verbindung zu Ihren REST-Services herzustellen. Falls die REST-Services nicht immer reagieren, müssen Sie die Einstellungen für das Verbindungszeitlimit zwischen Business Space und Ihren REST-Services aktualisieren, je nachdem, wie die Leistung auf den Servern für die REST-Services ist. Weitere Informationen enthält der Abschnitt Einstellung für die Zeitlimitüberschreitung für den Business Space-Ajax-Proxy ändern.

### **Business Space-Profil erstellen:**

Um Business Space-Profile zu erstellen oder zu erweitern, können Sie entweder das Profile Management Tool oder das Befehlszeilendienstprogramm manageprofiles

verwenden. Profile sind Gruppen von Dateien, die die Laufzeitumgebung für einen Deployment Manager, einen verwalteten Knoten oder einen eigenständigen Server definieren.

Wenn Business Space im Rahmen Ihres Produktprofils konfiguriert wird, sind diese Tasks optional.

*Business Space-Profil für eine eigenständige Konfiguration erstellen:*

Um Business Space-Profil für eine eigenständige Umgebung zu erstellen, können Sie entweder das Profile Management Tool oder das Befehlszeilendienstprogramm `manageprofiles` verwenden.

Wenn Business Space im Rahmen Ihres Produktprofils konfiguriert wird, sind diese Tasks optional.

*Business Space-Profil mithilfe des Profile Management Tool für eine eigenständige Konfiguration erstellen:*

Sie können das Profile Management Tool verwenden, um eigenständige Profile für Business Space zu erstellen.




- Überprüfen Sie die vollständige Liste der Voraussetzungen für das Erstellen oder Erweitern eines Profils, die unter Profilkonzepte im Information Center von WebSphere Application Server aufgeführt ist.
- Wenn Sie das Profile Management Tool mit der grafischen Benutzerschnittstelle Motif auf einem Solaris-Betriebssystem verwenden, kann es vorkommen, dass die Standardgröße des Profile Management Tool zu klein ist, um alle Nachrichten und Schaltflächen des Profile Management Tool anzuzeigen.
- Wenn Sie beabsichtigen, eine Datenbankentwurfsdatei für die Business Space-Datenbankinformationen zu verwenden, führen Sie die Schritte in „Eigenschaftendatei für Business Space-Datenbankentwurf erstellen“ auf Seite 254 aus.

Mit diesem Verfahren können Sie ein Business Space-Profil für eine eigenständige Konfiguration erstellen. Die Schritte beschreiben die Profilerstellungsoptionen 'Erweiterte Profilerstellung' und 'Typische Profilerstellung'.

Wenn Business Space im Rahmen Ihres Produktprofils konfiguriert wird, ist diese Task optional.

1. Starten Sie das Profile Management Tool.

Verwenden Sie einen der folgenden Befehle:

-   `installationsstammverz/bin/ProfileManagement/pmt.sh`
-  `installationsstammverz\bin\ProfileManagement\pmt.bat`

Die Seite 'Willkommen' wird angezeigt.

2. Klicken Sie auf der Seite 'Willkommen' auf die Schaltfläche **Profile Management Tool starten** oder auf die Registerkarte 'Profile Management Tool'.

Die Registerkarte 'Profile' wird angezeigt.

In der Registerkarte 'Profile' wird eine Liste der Profile angezeigt, die auf der Maschine erstellt wurden. Sie können das Profile Management Tool verwenden, um neue Profile zu erstellen oder vorhandene Profile zu erweitern.

3. Klicken Sie in der Registerkarte 'Profile' auf die Schaltfläche **Erstellen**.

Die Seite 'Umgebungsauswahl' wird in einem separaten Fenster geöffnet.




4. Wählen Sie auf der Seite 'Umgebungsauswahl' die Option **Eigenständiges Profil** aus und klicken Sie auf **Weiter**.
5. Entscheiden Sie auf der Seite 'Profileroptionsmöglichkeiten', ob das eigenständige Profil mithilfe der Option **Typische Profilerstellung** oder **Erweiterte Profilerstellung** erstellt werden soll.
6. Wenn Sie die Option **Typische Profilerstellung** gewählt haben, führen Sie folgende Schritte aus:
  - a. Geben Sie auf der Seite 'Verwaltungssicherheit' Werte für Benutzernamen und Kennwort ein, bestätigen Sie das Kennwort und klicken Sie auf **Weiter**. Alle Profileinstellungen, einschließlich Profilooptionen und Datenbanken, werden standardmäßig konfiguriert und auf der Seite 'Profilzusammenfassung' angezeigt.
  - b. Klicken Sie auf der Seite 'Profil - Zusammenfassung' auf die Option **Erstellen**, um das Profil zu erstellen, oder klicken Sie auf **Zurück**, um die Merkmale für das Profil zu ändern.

Der Fortschritt der Profilkonfiguration wird in einem eigenen Fenster angezeigt. Wenn die Profilerstellung abgeschlossen ist, wird eine Seite mit der Nachricht **Das Profile Management Tool hat das Profil erfolgreich erstellt** angezeigt.

**Achtung:** Wenn Fehler bei der Profilerstellung festgestellt wurden, werden anstelle der Nachricht zur erfolgreichen Profilerstellung möglicherweise andere Nachrichten angezeigt, wie z. B.:

- **Das Profile Management Tool hat das Profil erstellt, wobei jedoch Fehler aufgetreten sind.** Diese Nachricht gibt an, dass die Profilerstellung zwar durchgeführt wurde, aber Fehler generiert wurden.
- **Das Profile Management Tool kann das Profil nicht erstellen.** Diese Nachricht gibt an, dass die Profilerstellung vollständig fehlgeschlagen ist.

Auf der Seite zur Fertigstellung des Profils wird zur Fehlerbehebung auf die Protokolldatei verwiesen.

7. Wenn Sie die Option **Erweiterte Profilerstellung** gewählt haben, führen Sie folgende Schritte aus:
  - a. Wählen Sie auf der Seite 'Optionale Anwendungsimplementierung' die Kontrollkästchen aus, wenn Sie die Administrationskonsole und die Standardanwendung implementieren wollen.
  - b. Führen Sie auf der Seite 'Profilname und -position' die folgenden Schritte aus:
    - 1) Geben Sie einen eindeutigen Namen an oder übernehmen Sie den Standardwert. Sie müssen jedem Profil, das Sie erstellen, einen Namen zuweisen. Wenn Sie mehrere Profile verwenden, können Sie die Profile anhand des Namens auf ihrer höchsten Ebene unterscheiden. Wenn Sie nicht den Standardnamen verwenden, wählen Sie bei Windows einen kurzen Namen, da die Länge der Pfadnamen begrenzt ist.
    - 2) Geben Sie im Feld 'Profilverzeichnis' das Verzeichnis für das Profil ein oder verwenden Sie die Schaltfläche 'Durchsuchen', um zum Profilverzeichnis zu wechseln. Das von Ihnen angegebene Verzeichnis enthält dann die Dateien, die die Laufzeitumgebung definieren (Befehle, Konfigurationsdateien, Protokolldateien usw.). Welches Verzeichnis standardmäßig verwendet wird, hängt von Ihrem Betriebssystem ab:
      -  **Linux**  **UNIX** `installationsstammverz/profiles/profilname`
      -  **Windows** `installationsstammverz\profiles\profilname`

Dabei ist *profilname* der von Ihnen angegebene Name.

Das Feld für das Profilverzeichnis muss folgende Bedingungen erfüllen:

- Der *profilname* muss eindeutig sein.
- Das von Ihnen angegebene Verzeichnis muss leer sein.
- Ihre Benutzer-ID muss für das Verzeichnis berechtigt sein.
- Für die Erstellung des Profils muss ausreichend Speicherplatz vorhanden sein.

- 3) Optional: Sie können das Profil, das Sie erstellen, als Standardprofil definieren, sodass es von Befehlen automatisch verwendet wird. Wählen Sie hierzu das Kontrollkästchen **Dieses Profil als Standardprofil verwenden** aus. Dieses Kontrollkästchen wird nur angezeigt, wenn sich auf Ihrem System ein Profil befindet.

Beim Standardprofil funktionieren die Befehle automatisch. Das erste Profil, das Sie auf einer Workstation erstellen, ist das Standardprofil. Das Standardprofil ist das Standardziel für Befehle, die im Unterverzeichnis 'bin' des Installationsverzeichnisses eingegeben werden. Ist auf einer Workstation nur ein Profil vorhanden, dann wird jeder Befehl für dieses Profil ausgeführt. Bei Vorhandensein von mehr als einem Profil müssen Sie bei bestimmten Befehlen das Profil angeben, auf das sich der Befehl bezieht.

- 4) Klicken Sie auf **Weiter**.

- c. Führen Sie auf der Seite mit den Namen für Knoten und Host die folgenden Aktionen für das Profil durch, das Sie erstellen:

- Geben Sie im Feld 'Knotenname' einen Namen für den Knoten ein oder übernehmen Sie den Standardwert. Wählen Sie einen möglichst kurzen Knotennamen, aber stellen Sie sicher, dass jeder Knotenname in Ihrer Implementierungsumgebung eindeutig ist.
- Geben Sie im Feld 'Hostname' einen Namen für den Host ein oder übernehmen Sie den Standardwert.
- Geben Sie im Feld 'Zellenname' einen Namen für die Zelle ein oder übernehmen Sie den Standardwert.

Klicken Sie auf **Weiter**, um die Seite 'Verwaltungssicherheit' anzuzeigen.

- d. Geben Sie auf der Seite 'Verwaltungssicherheit' Werte für Benutzernamen und Kennwort ein und bestätigen Sie das Kennwort. Klicken Sie auf **Weiter**.

- e. Geben Sie auf der Seite 'Sicherheitszertifikat (Teil 1)' an, ob Sie neue Zertifikate erstellen oder vorhandene Zertifikate importieren möchten. Führen Sie folgende Aktionen durch:

- Um ein neues persönliches Standardzertifikat und ein neues Stammsignaturzertifikat zu erstellen, wählen Sie **Neues persönliches Standardzertifikat erstellen** und **Neues Stammsignaturzertifikat erstellen** aus und klicken Sie auf **Weiter**.
- Um vorhandene Zertifikate zu importieren, wählen Sie **Vorhandenes persönliches Standardzertifikat importieren** und **Vorhandenes Stammsignaturzertifikat importieren** aus und geben Sie folgende Informationen an:
  - Geben Sie im Feld 'Pfad' den Verzeichnispfad zu dem vorhandenen Zertifikat ein.
  - Geben Sie im Feld 'Kennwort' das Kennwort für das Zertifikat ein.
  - Wählen Sie im Feld 'Keystore-Typ' den Keystore-Typ für das zu importierende Zertifikat aus.

- Wählen Sie im Feld 'Keystore-Alias' das Keystore-Alias für das zu importierende Zertifikat aus.
- Klicken Sie auf **Weiter**.

Wenn Sie ein persönliches Zertifikat als persönliches Standardzertifikat importieren, importieren Sie das Stammzertifikat, mit dem das persönliche Zertifikat signiert wurde. Andernfalls fügt das Profile Management Tool den Unterzeichner des persönlichen Zertifikats zur Datei `trust.p12` hinzu. Geben Sie beim Importieren des persönlichen Standardzertifikats oder des Stammsignaturzertifikats den Pfad und das Kennwort an und wählen Sie den Keystore-Typ und das Keystore-Alias für jedes Zertifikat aus, das Sie importieren.

- f. Prüfen Sie auf der Seite 'Sicherheitszertifikat (Teil 1)', ob die Zertifikatsinformationen richtig sind, und klicken Sie auf **Weiter**, um die Seite für die Portwertzuordnung anzuzeigen.

Wenn Sie die Zertifikate erstellen, können Sie entweder die Standardwerte übernehmen oder die Werte für die Erstellung neuer Zertifikate ändern. Ein persönliches Standardzertifikat hat eine Standardgültigkeit von einem Jahr und wird vom Stammsignaturzertifikat signiert. Das Stammsignaturzertifikat ist ein selbst signiertes Zertifikat mit einer Standardgültigkeit von 15 Jahren. Das Keystore-Standardkennwort für das Stammsignaturzertifikat lautet `WebAS`. Ändern Sie dieses Kennwort. Das neue Kennwort darf keine Zeichen des Doppelbytezeichensatzes (DBCS) enthalten, da bestimmte Keystore-Typen, unter anderem auch PKCS12, diese Zeichen nicht unterstützen. Welche Keystore-Typen unterstützt werden, hängt von den Providern in der Datei `java.security` ab.

Wenn Sie ein oder beide Zertifikate erstellen oder ein oder beide Zertifikate importieren, werden die folgenden Keystore-Dateien erstellt:

- `key.p12`: Enthält das persönliche Standardzertifikat.
- `trust.p12`: Enthält das Unterzeichnerzertifikat vom Standardstammzertifikat.
- `root-key.p12`: Enthält das Stammsignaturzertifikat.
- `default-signers.p12`: Enthält Unterzeichnerzertifikate, die zu allen neuen Keystore-Dateien hinzugefügt werden, die Sie nach der Installation und Inbetriebnahme des Servers erstellt haben. Standardmäßig enthält die Keystore-Datei das Unterzeichnerzertifikat für das Standardstammzertifikat und ein DataPower<sup>®</sup>-Unterzeichnerzertifikat.
- `deleted.p12`: Enthält Zertifikate, die mit der Task 'deleteKeyStore' gelöscht wurden und bei Bedarf wiederhergestellt werden können.
- `1tpa.jceks`: Enthält LTPA-Standardschlüssel (LTPA = Lightweight Third-Party Authentication) für Server, die die Server in Ihrer Umgebung verwenden, um miteinander zu kommunizieren.

Alle diese Dateien besitzen dasselbe Kennwort, wenn Sie die Zertifikate erstellen oder importieren. Hierbei handelt es sich entweder um das Standardkennwort oder um ein von Ihnen angegebene Kennwort. Ein importiertes Zertifikat wird zur Datei `key.p12` oder zur Datei `root-key.p12` hinzugefügt. Wenn Sie Zertifikate importieren und diese Zertifikate nicht die gewünschten Informationen enthalten, klicken Sie auf **Zurück**, um ein anderes Zertifikat zu importieren.

- g. Prüfen Sie auf der Seite für die Portwertzuordnung, ob die für das Profil angegebenen Ports eindeutig sind, und klicken Sie auf **Weiter**.


Das Profile Management Tool ermittelt Ports, die momentan von anderen IBM WebSphere-Produkten verwendet werden, und zeigt die empfohlenen

Portwerte an, die keine Konflikte mit den bereits vorhandenen Werten verursachen. Wenn andere Anwendungen die angegebenen Ports verwenden, dann stellen Sie sicher, dass dadurch keine Konflikte verursacht werden. Wenn Sie sich dafür entscheiden, die Administrationskonsole im Fenster 'Optionale Anwendungsimplementierung' nicht zu implementieren, dann sind die Ports der Administrationskonsole in der Anzeige für die Portwertzuordnung nicht verfügbar. Ports werden als belegt erkannt, wenn sie einem Profil zugeordnet sind, das unter einer Installation erstellt wurde, die vom derzeitigen Benutzer durchgeführt wird, oder wenn sie momentan belegt sind.

Obwohl das Tool die Ports überprüft, wenn Sie die Seite für die Portwertzuordnung öffnen, können trotzdem Portkonflikte auftreten. Diese werden durch die Auswahl verursacht, die Sie auf den nachfolgenden Seiten des Profile Management Tool treffen. Ports werden erst zugeordnet, wenn die Profilerstellung abgeschlossen ist. Wenn Sie einen Portkonflikt vermuten, können Sie nach der Profilerstellung prüfen, ob ein solcher vorliegt.

Ermitteln Sie die bei der Profilerstellung verwendeten Ports, indem Sie die folgende Datei überprüfen: `profile_root/properties/portdef.props`. In dieser Datei befinden sich die Schlüssel und Werte, die für die Definition der Ports verwendet wurden. Wenn Sie auf einen Portkonflikt stoßen, können Sie die Zuordnung von Ports manuell ändern. Informationen zur erneuten Zuordnung von Ports finden Sie unter Ports in vorhandenen Profilen aktualisieren im Information Center zu WebSphere Application Server Network Deployment. Führen Sie wie in diesem Abschnitt erläutert die Datei `updatePorts.ant` anhand des Scripts `ws_ant` aus.

- h. Wenn Sie auf einer Linux- oder Windows-Plattform installieren und wenn Sie über die Rootberechtigung oder das Zugriffsrecht für Administratorgruppen verfügen, wird die Seite für die Linux- bzw. Windows-Servicedefinition angezeigt. Geben Sie auf der Seite 'Servicedefinition' an, ob der Prozessserver unter einem Windows-Service (in der Windows-Terminologie ein 'Windows-Dienst') oder unter einem Linux-Service ausgeführt wird, und klicken Sie auf **Weiter**, um die Seite **Web Server Definition** anzuzeigen.

 Die Anzeige für die Windows-Servicedefinition wird für die Windows-Plattform nur angezeigt, wenn die ID, mit der der Windows-Service installiert wird, über das Zugriffsrecht für Administratorgruppen verfügt. Wenn Sie das Profil als Windows-Service konfigurieren, startet das Produkt für alle Prozesse, die mit dem Befehl **startServer** oder **startManager** gestartet werden, einen Windows-Service. Wenn Sie z. B. einen Server oder Deployment Manager als Windows-Service konfigurieren und den Befehl **startServer** oder **startManager** eingeben, startet der Befehl **wasservice** die definierten Services.

**Wichtig:** Wenn Sie sich mit einem angegebenen Benutzeraccount anmelden wollen, müssen Sie die Benutzer-ID und das Kennwort für den Benutzer, der den Service ausführen soll, sowie den Starttyp (Standardwert ist Manuell) angeben. Der Name der Benutzer-ID darf keine Leerzeichen enthalten. Die Benutzer-ID muss der Administratorgruppe angehören und die erweiterten Benutzerberechtigungen 'Als Dienst anmelden' und 'Einsetzen als Teil des Betriebssystems' besitzen. Sofern die Benutzer-ID der Administratorgruppe angehört, erteilt ihr das Profile Management Tool die erweiterte Benutzerberechtigung automatisch, falls diese ID noch nicht über die erweiterte Benutzerberechtigung verfügt. Sie können den Windows-Service, der bei der Profilerstellung hinzugefügt wurde, beim Löschen des Profils entfernen.



**Windows** **Hinweise zu IPv6, wenn Profile als Windows-Services ausgeführt werden:** Profile, die für die Ausführung als Windows-Service erstellt wurden, können bei Verwendung von IPv6 nicht gestartet werden, wenn der Service für die Ausführung als lokales System konfiguriert wurde. Erstellen Sie eine benutzerspezifische Umgebungsvariable, um IPv6 zu aktivieren. Da es sich bei dieser Umgebungsvariablen um eine Benutzervariable und nicht um eine Variable des lokalen Systems handelt, kann nur ein Windows-Service, der unter der ID des jeweiligen Benutzers ausgeführt wird, auf diese Umgebungsvariable zugreifen. Standardmäßig wird der Service so definiert, dass er als lokales System ausgeführt wird, wenn ein neues Profil erstellt und für die Ausführung als Windows-Service konfiguriert wird. Wenn Sie versuchen, den Windows-Service auszuführen, kann dieser Service nicht auf die Benutzerumgebungsvariable zugreifen, die für IPv6 definiert ist. Er wird daher als IPv4-Service gestartet. Der Server wird in diesem Fall nicht ordnungsgemäß gestartet. Um das Problem zu beheben, müssen Sie bei der Profilerstellung angeben, dass der Windows-Service nicht als lokales System ausgeführt werden soll, sondern unter derselben Benutzer-ID, unter der die Umgebungsvariable für IPv6 definiert ist.

**Linux** Die Anzeige für die Linux-Servicedefinition wird nur aufgerufen, wenn das aktuelle Betriebssystem eine unterstützte Version von Linux ist und der aktuelle Benutzer über die erforderlichen Berechtigungen verfügt. Ihr Produkt versucht, Linux-Services für Prozesse zu starten, die mit dem Befehl **startServer** oder **startManager** gestartet wurden. Wenn Sie z. B. einen Server oder Deployment Manager als Linux-Service konfigurieren und den Befehl **startServer** oder **startManager** eingeben, startet der Befehl **wasservice** die definierten Services. Standardmäßig wird Ihr Produkt nicht als Linux-Service ausgeführt. Für die Erstellung des Service muss der Benutzer, der das Profile Management Tool ausführt, ein Rootbenutzer sein. Wenn Sie das Profile Management Tool mit einer Benutzer-ID ohne Rootberechtigung ausführen, wird die Anzeige für die Linux-Servicedefinition nicht geöffnet und es wird auch kein Service erstellt. Sie müssen einen Benutzernamen angeben, unter dem der Service ausgeführt wird. Um einen Linux-Service zu löschen, muss der Benutzer der Root sein oder über die entsprechende Berechtigung zum Löschen des Service verfügen. Ansonsten wird ein Script zum Entfernen erstellt, das der Root zum Löschen des Service anstelle des Benutzers verwenden kann.

- i. Wenn Sie unter einem anderen Betriebssystem oder als Benutzer ohne Rootberechtigung unter einem Linux- oder Windows-Betriebssystem installieren, wird die Seite **Web Server Definition** angezeigt. Führen Sie zum Einschließen einer Web-Server-Definition in das Profil die folgenden Schritte aus:
  - 1) Wählen Sie das Kontrollkästchen **Web-Server-Definition erstellen** aus.
  - 2) Geben Sie auf der Seite die Merkmale des Web-Servers an und klicken Sie auf **Weiter**.
  - 3) Geben Sie im zweiten Teil der Seite die Merkmale des Web-Servers an.

Wenn Sie einen Web-Server verwenden, um Anforderungen an Ihren Server weiterzuleiten, müssen Sie eine Web-Server-Definition angeben. Sie können diese Definition entweder direkt einschließen oder den Web-Server zu einem späteren Zeitpunkt für Business Space definieren. Wenn Sie die Web-Server-Definition während der Erstellung dieses Profils definieren, können Sie den Web-Server und das zugehörige Plug-in nach der Profilerstellung installieren. Sie müssen jedoch beide in den Pfaden installieren, die Sie auf den Seiten für die Web-Server-Definition angeben



haben. Wenn Sie den Web-Server nach der Erstellung dieses Profils für Business Space definieren, müssen Sie für die Definition ein separates Profil verwenden.

- 4) Klicken Sie auf **Weiter**.
- j. Wenn Sie eine Datenbankentwurfsdatei verwenden wollen, die Sie bereits erstellt haben, um die Datenbanken zu konfigurieren, führen Sie die folgenden Schritte aus, anstatt die Datenbankkonfigurationseiten zu verwenden.
  - 1) Wählen Sie **Datenbankentwurfsdatei verwenden** für die Datenbankkonfiguration aus.
  - 2) Klicken Sie auf **Durchsuchen**.
  - 3) Geben Sie den vollständig qualifizierten Pfadnamen für die Entwurfsdatei an.
  - 4) Klicken Sie auf **Weiter**.
- k. Wenn Sie keine Datenbankentwurfsdatei verwendet haben, führen Sie auf der Seite 'Datenbankkonfiguration' folgende Aktionen durch:
  - 1) Wählen Sie aus der Liste **Datenbankprodukt auswählen** das Datenbankprodukt aus, das von dem Profil verwendet werden soll.
  - 2) Wählen Sie das Kontrollkästchen **Standardausgabeverzeichnis für Datenbankscripts außer Kraft setzen** aus, wenn Sie das Verzeichnis festlegen wollen, in das die SQL-Scripts zur Erstellung der Datenbanktabellen geschrieben werden. Wenn Sie das Kontrollkästchen nicht auswählen, werden die Scripts in das Standardverzeichnis ausgegeben.
  - 3) Klicken Sie auf **Weiter**, um die Seite 'Datenbankkonfiguration (Teil 2)' anzuzeigen.

Die auf der Seite 'Datenbankkonfiguration (Teil 2)' angezeigten Informationen hängen von dem Wert ab, der in der Liste 'Datenbankprodukt auswählen' auf der Seite 'Datenbankkonfiguration' angegeben wurde.

- l. Nehmen Sie die Datenbankkonfiguration auf der Seite 'Datenbankkonfiguration (Teil 2)' vor. Abhängig von Ihrem Datenbankprodukt müssen Sie eventuell einen Benutzernamen und ein Kennwort für zur Authentifizierung bei der Datenbank sowie die JDBC-Treiberinformationen, Host, Port und Schema eingeben.
- m. Klicken Sie auf der Seite 'Profil - Zusammenfassung' auf die Option **Erstellen**, um das Profil zu erstellen, oder klicken Sie auf **Zurück**, um die Merkmale für das Profil zu ändern.

Der Fortschritt der Profilkonfiguration wird in einem eigenen Fenster angezeigt. Wenn die Profilerstellung abgeschlossen ist, wird eine Seite mit der Nachricht **Das Profile Management Tool hat das Profil erfolgreich erstellt** angezeigt.

**Achtung:** Wenn Fehler bei der Profilerstellung festgestellt wurden, werden anstelle der Nachricht zur erfolgreichen Profilerstellung möglicherweise andere Nachrichten angezeigt, wie z. B.:

- **Das Profile Management Tool hat das Profil erstellt, wobei jedoch Fehler aufgetreten sind.** Diese Nachricht gibt an, dass die Profilerstellung zwar durchgeführt wurde, aber Fehler generiert wurden.
- **Das Profile Management Tool kann das Profil nicht erstellen.** Diese Nachricht gibt an, dass die Profilerstellung vollständig fehlgeschlagen ist.

Auf der Seite zur Fertigstellung des Profils wird zur Fehlerbehebung auf die Protokolldatei verwiesen.

*Business Space-Profil mithilfe des Befehlszeilendienstprogramms manageprofiles für eine eigenständige Konfiguration erstellen:*

Mit dem Befehlszeilendienstprogramm manageprofiles können Sie Business Space-Profil für Ihre eigenständige Business Space-Serverkonfiguration erstellen.

Stellen Sie vor der Ausführung des Befehlszeilendienstprogramms manageprofiles sicher, dass Sie die folgenden Tasks vollständig ausgeführt haben:

- Überprüfen Sie die vollständige Liste der Voraussetzungen für das Erstellen oder Erweitern eines Profils, die unter Profilkonzepte im Information Center von WebSphere Application Server aufgeführt ist.
- Schauen Sie sich die Beispiele mit Befehlen zur Profilerstellung an.
- Vergewissern Sie sich, dass das Befehlszeilendienstprogramm manageprofiles nicht bereits für dasselbe Profil ausgeführt wird. Wenn Sie eine Fehlermeldung erhalten, prüfen Sie, ob gleichzeitig noch eine weitere Profilerstellung oder Profilerweiterung durchgeführt wird. Wenn dies der Fall ist, müssen Sie auf den Abschluss dieser Erstellung bzw. Erweiterung warten.

Diese Task beschreibt, wie Sie mit dem Befehlszeilendienstprogramm manageprofiles Business Space-Profil für Ihre eigenständige Business Space-Konfiguration erstellen können. Führen Sie die folgenden Schritte aus, um das Befehlszeilendienstprogramm manageprofiles zum Erstellen eines Profils zu verwenden.

1. Lokalisieren Sie die Profilschablone default.bspace für eigenständige Profile (Business Space), die eigenständige Server definieren.

Im Verzeichnis *installationsstammverzeichnis/profileTemplates/BusinessSpace* finden Sie Schablonen für die einzelnen Profile.

2. Ermitteln Sie im Abschnitt „Befehlszeilendienstprogramm 'manageprofiles' (für Business Space-Profil)“ auf Seite 224, welche Parameter für die Profilerstellung erforderlich sind. Ermitteln Sie die Werte, die Sie für das Profil angeben möchten. Überprüfen Sie hierzu die Standardwerte, um festzustellen, ob diese bedarfsgerecht für Ihr Profil sind. Beispielsweise können Sie folgende Parameter verwenden: `-templatePath`, `-enableAdminSecurity`, `-adminUserName`, `-adminPassword`, `-dbType`, `-dbUserId`, `-dbPassword`, `-dbJDBCClasspath`, `-dbName`, `-bspaceSchema`, `-dbHostName`, `-dbServerPort` und `-dbDelayConfig`.

Stellen Sie bei der Verwendung einer Windows-Authentifizierung mit Microsoft SQL Server sicher, dass der Parameter `-dbWinAuth` als `true` gesetzt ist.

3. Führen Sie die Datei von der Befehlszeile aus. Im Folgenden finden Sie ein einfaches Beispiel:

```
manageProfiles -create -templatePath installationsstammverzeichnis/profileTemplates/BusinessSpace
-enableAdminSecurity true -adminUserName administratorname -adminPassword administratorname
-dbType DB2_Universal -dbUserId db2-benutzer-id -dbPassword db2-benutzername
-dbJDBCClasspath installationsstammverzeichnis/jdbcdrivers/DB2 -dbName datenbankname -bspaceSchema
datenbankschemaname -dbHostName hostname -dbServerPort portnummer -dbDelayConfig false
```

Der Befehl zeigt bei seiner Ausführung den aktuellen Status an. Warten Sie, bis er beendet ist. Für die Datei gilt die normale Syntaxprüfung und die Datei wird wie jede andere Antwortdatei syntaktisch analysiert. Einzelwerte in der Antwortdatei werden als Befehlszeilenparameter behandelt.

*Business Space-Profil für eine Network Deployment-Konfiguration erstellen:*

Um Business Space-Profil für eine Network Deployment-Umgebung zu erstellen, können Sie entweder das Profile Management Tool oder das Befehlszeilendienstprogramm manageprofiles verwenden.

Wenn Business Space im Rahmen Ihres Produktprofils konfiguriert wird, sind diese Tasks optional.

*Business Space-Profil mithilfe von Profile Management Tool für eine Network Deployment-Konfiguration erstellen:*

Sie können das Profile Management Tool verwenden, um Business Space-Profile für eine Network Deployment-Konfiguration zu erstellen: Sie erstellen ein Network Deployment-Profil und angepasste Profile (verwaltete Knoten).

- Überprüfen Sie die vollständige Liste der Voraussetzungen für das Erstellen oder Erweitern eines Profils, die unter Profilkonzepte im Information Center von WebSphere Application Server aufgeführt ist.
- Wenn Sie das Profile Management Tool mit der grafischen Benutzerschnittstelle Motif auf einem Solaris-Betriebssystem verwenden, kann es vorkommen, dass die Standardgröße des Profile Management Tool zu klein ist, um alle Nachrichten und Schaltflächen des Profile Management Tool anzuzeigen.




Mit diesem Verfahren können Sie ein Business Space-Profil für eine Network Deployment-Konfiguration erstellen. Sie erstellen ein Deployment Manager-Profil und angepasste Profile für verwaltete Knoten. Die Schritte beschreiben die Profilerstellungsoptionen 'Erweiterte Profilerstellung' und 'Typische Profilerstellung'.

Wenn Business Space im Rahmen Ihres Produktprofils konfiguriert wird, ist diese Task optional.

1. Erstellen Sie das Deployment Manager-Profil.

a. Starten Sie das Profile Management Tool.

Verwenden Sie einen der folgenden Befehle:

-   `installationsstammverz/bin/ProfileManagement/pmt.sh`
-  `installationsstammverz\bin\ProfileManagement\pmt.bat`

b. Klicken Sie auf der Seite 'Willkommen' auf die Schaltfläche **Profile Management Tool starten** oder auf die Registerkarte 'Profile Management Tool'.

Die Registerkarte 'Profile' wird angezeigt.

In der Registerkarte 'Profile' wird eine Liste der Profile angezeigt, die auf der Maschine erstellt wurden. Sie können das Profile Management Tool verwenden, um neue Profile zu erstellen oder vorhandene Profile zu erweitern.

c. Klicken Sie in der Registerkarte 'Profile' auf die Schaltfläche **Erstellen**.

Die Seite 'Umgebungsauswahl' wird in einem separaten Fenster geöffnet.

d. Erweitern Sie auf der Seite 'Umgebungsauswahl' den Abschnitt **Business Space powered by WebSphere**, wählen Sie die Option **Deployment Manager für Business Space powered by WebSphere** und klicken Sie auf **Weiter**.

e. Entscheiden Sie auf der Seite 'Profilerstellungsoptionen', ob das eigenständige Profil mithilfe der Option **Typische Profilerstellung** oder **Erweiterte Profilerstellung** erstellt werden soll.

f. Wenn Sie die Option **Typische Profilerstellung** gewählt haben, führen Sie folgende Schritte aus:

- 1) Geben Sie auf der Seite 'Verwaltungssicherheit' Werte für Benutzernamen und Kennwort ein, bestätigen Sie das Kennwort und klicken Sie auf **Weiter**. Alle Profileinstellungen, einschließlich Profilooptionen und Datenbanken, werden standardmäßig konfiguriert und auf der Seite 'Profilzusammenfassung' angezeigt.




- 2) Klicken Sie auf der Seite 'Profil - Zusammenfassung' auf die Option **Erstellen**, um das Profil zu erstellen, oder klicken Sie auf **Zurück**, um die Merkmale für das Profil zu ändern.

Der Fortschritt der Profilkonfiguration wird in einem eigenen Fenster angezeigt. Wenn die Profilerstellung abgeschlossen ist, wird eine Seite mit der Nachricht **Das Profile Management Tool hat das Profil erfolgreich erstellt**. angezeigt.

**Achtung:** Wenn Fehler bei der Profilerstellung festgestellt wurden, werden anstelle der Nachricht zur erfolgreichen Profilerstellung möglicherweise andere Nachrichten angezeigt, wie z. B.:

- **Das Profile Management Tool hat das Profil erstellt, wobei jedoch Fehler aufgetreten sind.**
- **Das Profile Management Tool kann das Profil nicht erstellen.**

Auf der Seite zur Fertigstellung des Profils wird zur Fehlerbehebung auf die Protokolldatei verwiesen.

- g. Wenn Sie die Option **Erweiterte Profilerstellung** gewählt haben, führen Sie folgende Schritte aus:
- 1) Wählen Sie auf der Seite 'Optionale Anwendungsimplementierung' die Kontrollkästchen aus, wenn Sie die Administrationskonsole und die Standardanwendung implementieren wollen.
  - 2) Führen Sie auf der Seite 'Profilname und -position' die folgenden Schritte aus:
    - a) Geben Sie einen eindeutigen Namen an oder übernehmen Sie den Standardwert. Sie müssen jedem Profil, das Sie erstellen, einen Namen zuweisen. Wenn Sie mehrere Profile verwenden, können Sie sie anhand dieses Namens auseinanderhalten. Wenn Sie nicht den Standardnamen verwenden, wählen Sie bei Windows einen kurzen Namen, da die Länge der Pfadnamen begrenzt ist.
    - b) Geben Sie im Feld 'Profilverzeichnis' das Verzeichnis für das Profil ein oder verwenden Sie die Schaltfläche 'Durchsuchen', um zum Profilverzeichnis zu wechseln. Das von Ihnen angegebene Verzeichnis enthält dann die Dateien, die die Laufzeitumgebung definieren (Befehle, Konfigurationsdateien, Protokolldateien usw.). Welches Verzeichnis standardmäßig verwendet wird, hängt vom verwendeten Betriebssystem ab:
      -   `installationsstammverz/profiles/  
profilname`
      -  `installationsstammverz\profiles\profilname`Dabei ist *profilname* der von Ihnen angegebene Name.
  - c) Optional: Sie können das Profil, das Sie erstellen, als Standardprofil definieren, sodass es von Befehlen automatisch verwendet wird. Wählen Sie hierzu das Kontrollkästchen **Dieses Profil als Standard-**

**profil verwenden** aus. Dieses Kontrollkästchen wird nur angezeigt, wenn sich auf Ihrem System ein Profil befindet.

Beim Standardprofil funktionieren die Befehle automatisch. Das erste Profil, das Sie auf einer Workstation erstellen, ist das Standardprofil. Das Standardprofil ist das Standardziel für Befehle, die im Unterverzeichnis 'bin' des Installationsverzeichnisses eingegeben werden. Ist auf einer Workstation nur ein Profil vorhanden, dann wird jeder Befehl für dieses Profil ausgeführt. Bei Vorhandensein von mehr als einem Profil müssen Sie bei bestimmten Befehlen das Profil angeben, auf das sich der Befehl bezieht.

- d) Klicken Sie auf **Weiter**.
- 3) Führen Sie auf der Seite mit den Namen für Knoten und Host die folgenden Aktionen für das Profil durch, das Sie erstellen:
- Geben Sie im Feld 'Knotenname' einen Namen für den Knoten ein oder übernehmen Sie den Standardwert. Wählen Sie einen möglichst kurzen Knotennamen, aber stellen Sie sicher, dass jeder Knotenname in Ihrer Implementierungsumgebung eindeutig ist.
  - Geben Sie im Feld 'Hostname' einen Namen für den Host ein oder übernehmen Sie den Standardwert.
  - Geben Sie im Feld 'Zellenname' einen Namen für die Zelle ein oder übernehmen Sie den Standardwert.

Klicken Sie auf **Weiter**, um die Seite 'Verwaltungssicherheit' anzuzeigen.

- 4) Geben Sie auf der Seite 'Verwaltungssicherheit' Werte für Benutzernamen und Kennwort ein und bestätigen Sie das Kennwort. Klicken Sie auf **Weiter**.
- 5) Geben Sie auf der Seite 'Sicherheitszertifikat (Teil 1)' an, ob Sie neue Zertifikate erstellen oder vorhandene Zertifikate importieren möchten. Führen Sie folgende Aktionen durch:
- Um ein neues persönliches Standardzertifikat und ein neues Stammsignaturzertifikat zu erstellen, wählen Sie **Neues persönliches Standardzertifikat erstellen** und **Neues Stammsignaturzertifikat erstellen** aus und klicken Sie auf **Weiter**.
  - Um vorhandene Zertifikate zu importieren, wählen Sie **Vorhandenes persönliches Standardzertifikat importieren** und **Vorhandenes Stammsignaturzertifikat importieren** aus und geben Sie folgende Informationen an:
    - Geben Sie im Feld 'Pfad' den Verzeichnispfad zu dem vorhandenen Zertifikat ein.
    - Geben Sie im Feld 'Kennwort' das Kennwort für das Zertifikat ein.
    - Wählen Sie im Feld 'Keystore-Typ' den Keystore-Typ für das zu importierende Zertifikat aus.
    - Wählen Sie im Feld 'Keystore-Alias' das Keystore-Alias für das zu importierende Zertifikat aus.
    - Klicken Sie auf **Weiter**.

Wenn Sie ein persönliches Zertifikat als persönliches Standardzertifikat importieren, importieren Sie das Stammzertifikat, mit dem das persönliche Zertifikat signiert wurde. Andernfalls fügt das Profile Management Tool den Unterzeichner des persönlichen Zertifikats zur Datei trust.p12 hinzu. Geben Sie beim Importieren des persönlichen Standardzertifikats oder des Stammsignaturzertifikats den Pfad und

das Kennwort an und wählen Sie den Keystore-Typ und das Keystore-Alias für jedes Zertifikat aus, das Sie importieren.

- 6) Prüfen Sie auf der Seite 'Sicherheitszertifikat (Teil 1)', ob die Zertifikatsinformationen richtig sind, und klicken Sie auf **Weiter**, um die Seite für die Portwertzuordnung anzuzeigen.

Wenn Sie die Zertifikate erstellen, können Sie entweder die Standardwerte übernehmen oder die Werte für die Erstellung neuer Zertifikate ändern. Ein persönliches Standardzertifikat hat eine Standardgültigkeit von einem Jahr und wird vom Stammsignaturzertifikat signiert. Das Stammsignaturzertifikat ist ein selbst signiertes Zertifikat mit einer Standardgültigkeit von 15 Jahren. Das Keystore-Standardkennwort für das Stammsignaturzertifikat lautet WebAS. Ändern Sie dieses Kennwort. Das neue Kennwort darf keine Zeichen des Doppelbytezeichensatzes (DBCS) enthalten, da bestimmte Keystore-Typen, unter anderem auch PKCS12, diese Zeichen nicht unterstützen. Welche Keystore-Typen unterstützt werden, hängt von den Providern in der Datei `java.security` ab.

Wenn Sie ein oder beide Zertifikate erstellen oder ein oder beide Zertifikate importieren, werden die folgenden Keystore-Dateien erstellt:

- `key.p12`: Enthält das persönliche Standardzertifikat.
- `trust.p12`: Enthält das Unterzeichnerzertifikat vom Standardstammzertifikat.
- `root-key.p12`: Enthält das Stammsignaturzertifikat.
- `default-signers.p12`: Enthält Unterzeichnerzertifikate, die zu allen neuen Keystore-Dateien hinzugefügt werden, die Sie nach der Installation und Inbetriebnahme des Servers erstellt haben. Standardmäßig enthält die Keystore-Datei das Unterzeichnerzertifikat für das Standardstammzertifikat und ein DataPower-Unterzeichnerzertifikat.
- `deleted.p12`: Enthält Zertifikate, die mit der Task 'deleteKeyStore' gelöscht wurden und bei Bedarf wiederhergestellt werden können.
- `ltpa.jceks`: Enthält LTPA-Standardschlüssel (LTPA = Lightweight Third-Party Authentication) für Server, die die Server in Ihrer Umgebung verwenden, um miteinander zu kommunizieren.

Alle diese Dateien besitzen dasselbe Kennwort, wenn Sie die Zertifikate erstellen oder importieren. Hierbei handelt es sich entweder um das Standardkennwort oder um ein von Ihnen angegebenes Kennwort. Ein importiertes Zertifikat wird zur Datei `key.p12` oder zur Datei `root-key.p12` hinzugefügt. Wenn Sie Zertifikate importieren und diese Zertifikate nicht die gewünschten Informationen enthalten, klicken Sie auf **Zurück**, um ein anderes Zertifikat zu importieren.

- 7) Prüfen Sie auf der Seite für die Portwertzuordnung, ob die für das Profil angegebenen Ports eindeutig sind, und klicken Sie auf **Weiter**.

Das Profile Management Tool ermittelt Ports, die momentan von anderen IBM WebSphere-Produkten verwendet werden, und zeigt die empfohlenen Portwerte an, die keine Konflikte mit den bereits vorhandenen Werten verursachen. Wenn andere Anwendungen die angegebenen Ports verwenden, dann stellen Sie sicher, dass dadurch keine Konflikte verursacht werden. Wenn Sie sich dafür entscheiden, die Administrationskonsole im Fenster 'Optionale Anwendungsimplementierung' nicht zu implementieren, dann sind die Ports der Administrationskonsole in der Anzeige für die Portwertzuordnung nicht verfügbar. Ports werden als belegt erkannt, wenn sie einem Profil zugeordnet sind, das unter einer Installation erstellt wurde, die vom derzeitigen Benutzer durchgeführt wird, oder wenn sie momentan belegt sind.



Obwohl das Tool die Ports überprüft, wenn Sie die Seite für die Portwertzuordnung öffnen, können trotzdem Portkonflikte auftreten. Diese werden durch die Auswahl verursacht, die Sie auf den nachfolgenden Seiten des Profile Management Tool treffen. Ports werden erst zugeordnet, wenn die Profilerstellung abgeschlossen ist. Wenn Sie einen Portkonflikt vermuten, können Sie nach der Profilerstellung prüfen, ob ein solcher vorliegt.

Ermitteln Sie die bei der Profilerstellung verwendeten Ports, indem Sie die folgende Datei überprüfen: `profile_root/properties/portdef.props`. In dieser Datei befinden sich die Schlüssel und Werte, die für die Definition der Ports verwendet wurden. Wenn Sie auf einen Portkonflikt stoßen, können Sie die Zuordnung von Ports manuell ändern. Informationen zur erneuten Zuordnung von Ports finden Sie unter Ports in vorhandenen Profilen aktualisieren im Information Center zu WebSphere Application Server Network Deployment. Führen Sie wie in diesem Abschnitt erläutert die Datei `updatePorts.ant` anhand des Scripts `ws_ant` aus.

- 8) Wenn Sie auf einer Linux- oder Windows-Plattform installieren und wenn Sie über die Rootberechtigung oder das Zugriffsrecht für Administratorgruppen verfügen, wird die Seite für die Linux- bzw. Windows-Service-Definition angezeigt. Geben Sie auf der Seite 'Service-Definition' an, ob ein Windows-Service (in der Windows-Terminologie ein 'Windows-Dienst') oder ein Linux-Service den Prozessserver ausführt, und klicken Sie auf **Weiter**, um die Seite **Web-Server-Definition** anzuzeigen.

**Windows** Die Anzeige für die Windows-Service-Definition wird für die Windows-Plattform nur angezeigt, wenn die ID, mit der der Windows-Service installiert wird, über das Zugriffsrecht für Administratorgruppen verfügt. Wenn Sie das Profil als Windows-Service konfigurieren, startet das Produkt für alle Prozesse, die mit dem Befehl `startServer` oder `startManager` gestartet werden, einen Windows-Service. Wenn Sie z. B. einen Server oder Deployment Manager als Windows-Service konfigurieren und den Befehl `startServer` oder `startManager` eingeben, startet der Befehl `wasservice` die definierten Services.

**Wichtig:** Wenn Sie sich mit einem angegebenen Benutzeraccount anmelden wollen, müssen Sie die Benutzer-ID und das Kennwort für den Benutzer, der den Service ausführen soll, sowie den Starttyp (Standardwert ist Manuell) angeben. Der Name der Benutzer-ID darf keine Leerzeichen enthalten. Die Benutzer-ID muss der Administratorgruppe angehören und die erweiterten Benutzerberechtigungen 'Als Dienst anmelden' und 'Einsetzen als Teil des Betriebssystems' besitzen. Sofern die Benutzer-ID der Administratorgruppe angehört, erteilt ihr das Profile Management Tool die erweiterte Benutzerberechtigung automatisch, falls diese ID noch nicht über die erweiterte Benutzerberechtigung verfügt. Sie können den Windows-Service, der bei der Profilerstellung hinzugefügt wurde, beim Löschen des Profils entfernen.

**Windows** **Hinweise zu IPv6, wenn Profile als Windows-Services ausgeführt werden:** Profile, die für die Ausführung als Windows-Service erstellt wurden, können bei Verwendung von IPv6 nicht gestartet werden, wenn der Service für die Ausführung als lokales System konfiguriert wurde. Erstellen Sie eine benutzerspezifische Umgebungsvariable, um IPv6 zu aktivieren. Da es sich bei dieser Umgebungsvariablen um eine Benutzervariable und nicht um eine Variable des lokalen Systems handelt, kann nur ein Windows-Service, der unter der ID des jeweiligen Be-

nutzers ausgeführt wird, auf diese Umgebungsvariable zugreifen. Standardmäßig wird der Service so definiert, dass er als lokales System ausgeführt wird, wenn ein neues Profil erstellt und für die Ausführung als Windows-Service konfiguriert wird. Wenn Sie versuchen, den Windows-Service auszuführen, kann dieser Service nicht auf die Benutzerumgebungsvariable zugreifen, die für IPv6 definiert ist. Er wird daher als IPv4-Service gestartet. Der Server wird in diesem Fall nicht ordnungsgemäß gestartet. Um das Problem zu beheben, müssen Sie bei der Profilerstellung angeben, dass der Windows-Service nicht als lokales System ausgeführt werden soll, sondern unter derselben Benutzer-ID, unter der die Umgebungsvariable für IPv6 definiert ist.

**Linux** Die Anzeige für die Linux-Servicedefinition wird nur aufgerufen, wenn das aktuelle Betriebssystem eine unterstützte Version von Linux ist und der aktuelle Benutzer über die erforderlichen Berechtigungen verfügt. Ihr Produkt versucht, Linux-Services für Serverprozesse zu starten, die mit dem Befehl `startServer` oder `startManager` gestartet wurden. Wenn Sie z. B. einen Server oder Deployment Manager als Linux-Service konfigurieren und den Befehl `startServer` oder `startManager` eingeben, startet der Befehl `wasservice` die definierten Services. Standardmäßig wird Ihr Produkt nicht als Linux-Service ausgeführt. Für die Erstellung des Service muss der Benutzer, der das Profile Management Tool ausführt, ein Rootbenutzer sein. Wenn Sie das Profile Management Tool mit einer Benutzer-ID ohne Rootberechtigung ausführen, wird die Anzeige für die Linux-Servicedefinition nicht geöffnet und es wird auch kein Service erstellt. Sie müssen einen Benutzernamen angeben, unter dem der Service ausgeführt wird. Um einen Linux-Service zu löschen, muss der Benutzer der Root sein oder über die entsprechende Berechtigung zum Löschen des Service verfügen. Ansonsten wird ein Script zum Entfernen erstellt, das der Root zum Löschen des Service anstelle des Benutzers verwenden kann.

- 9) Klicken Sie auf der Seite 'Profil - Zusammenfassung' auf die Option **Erstellen**, um das Profil zu erstellen, oder klicken Sie auf **Zurück**, um die Merkmale für das Profil zu ändern.

Der Fortschritt der Profilkonfiguration wird in einem eigenen Fenster angezeigt. Wenn die Profilerstellung abgeschlossen ist, wird eine Seite mit der Nachricht **Das Profile Management Tool hat das Profil erfolgreich erstellt.** angezeigt.

**Achtung:** Wenn Fehler bei der Profilerstellung festgestellt wurden, werden anstelle der Nachricht zur erfolgreichen Profilerstellung möglicherweise andere Nachrichten angezeigt, wie z. B.:

- **Das Profile Management Tool hat das Profil erstellt, wobei jedoch Fehler aufgetreten sind.**
- **Das Profile Management Tool kann das Profil nicht erstellen.**

Auf der Seite zur Fertigstellung des Profils wird zur Fehlerbehebung auf die Protokolldatei verwiesen.

2. Starten Sie das Deployment Manager-Profil.

Starten Sie den Deployment Manager mithilfe des Befehls `startServer` im Verzeichnis `profilstammverzeichnis/bin`.




Verwenden Sie die folgende Syntax:

- **Linux** `startServer.sh servername`
- **Windows** `startServer.bat servername`

Weitere Informationen zum Befehl `startServer` finden Sie im Abschnitt zum Befehl `startServer` im Information Center von WebSphere Application Server Version 8.0.

3. Erstellen Sie die angepassten (benutzerdefinierten) Profile (verwaltete Knoten).
  - a. Starten Sie das Profile Management Tool.

Verwenden Sie einen der folgenden Befehle:

    -   `installationsstammverz/bin/ProfileManagement/pmt.sh`
    -  `installationsstammverz\bin\ProfileManagement\pmt.bat`
  - b. Klicken Sie auf der Seite 'Willkommen' auf die Schaltfläche **Profile Management Tool starten** oder auf die Registerkarte 'Profile Management Tool'.

Die Registerkarte 'Profile' wird angezeigt.

In der Registerkarte 'Profile' wird eine Liste der Profile angezeigt, die auf der Maschine erstellt wurden. Sie können das Profile Management Tool verwenden, um neue Profile zu erstellen oder vorhandene Profile zu erweitern.
  - c. Klicken Sie in der Registerkarte 'Profile' auf die Schaltfläche **Erstellen**.




Die Seite 'Umgebungsauswahl' wird in einem separaten Fenster geöffnet.
  - d. Erweitern Sie auf der Seite 'Umgebungsauswahl' den Abschnitt **Business Space powered by WebSphere**, wählen Sie die Option **Angepasstes Profil (Business Space powered by WebSphere)** und klicken Sie auf **Weiter**.
  - e. Entscheiden Sie auf der Seite 'Profileroptionsmöglichkeiten', ob das eigenständige Profil mithilfe der Option **Typische Profilerstellung** oder **Erweiterte Profilerstellung** erstellt werden soll.
  - f. Wenn Sie die Option **Typische Profilerstellung** gewählt haben, führen Sie folgende Schritte aus:
    - 1) Auf der Seite 'Einbindung' können Sie auswählen, ob Sie den Knoten jetzt im Rahmen der Profilerstellung in den Deployment Manager einbinden oder ihn zu einem späteren Zeitpunkt und außerhalb der Profilerstellung mit dem Befehl `addNode` einbinden möchten. Wählen Sie das Kontrollkästchen **Diesen Knoten später einbinden** aus (bzw. inaktivieren Sie das Kontrollkästchen) und klicken Sie auf **Weiter**.
    - 2) Klicken Sie auf der Seite 'Profil - Zusammenfassung' auf die Option **Erstellen**, um das Profil zu erstellen, oder klicken Sie auf **Zurück**, um die Merkmale für das Profil zu ändern.

Der Fortschritt der Profilkonfiguration wird in einem eigenen Fenster angezeigt. Wenn die Profilerstellung abgeschlossen ist, wird eine Seite mit der Nachricht **Das Profile Management Tool hat das Profil erfolgreich erstellt** angezeigt.

**Achtung:** Wenn Fehler bei der Profilerstellung festgestellt wurden, werden anstelle der Nachricht zur erfolgreichen Profilerstellung möglicherweise andere Nachrichten angezeigt, wie z. B.:

    - **Das Profile Management Tool hat das Profil erstellt, wobei jedoch Fehler aufgetreten sind.**
    - **Das Profile Management Tool kann das Profil nicht erstellen.**

Auf der Seite zur Fertigstellung des Profils wird zur Fehlerbehebung auf die Protokolldatei verwiesen.
  - g. Wenn Sie die Option **Erweiterte Profilerstellung** gewählt haben, führen Sie folgende Schritte aus:

- 1) Führen Sie auf der Seite 'Profilname und -position' die folgenden Schritte aus:
  - a) Geben Sie einen eindeutigen Namen an oder übernehmen Sie den Standardwert. Sie müssen jedem Profil, das Sie erstellen, einen Namen zuweisen. Wenn Sie mehrere Profile verwenden, können Sie sie anhand dieses Namens auseinanderhalten. Wenn Sie nicht den Standardnamen verwenden, wählen Sie bei Windows einen kurzen Namen, da die Länge der Pfadnamen begrenzt ist.
  - b) Geben Sie im Feld 'Profilverzeichnis' das Verzeichnis für das Profil ein oder verwenden Sie die Schaltfläche 'Durchsuchen', um zum Profilverzeichnis zu wechseln. Das von Ihnen angegebene Verzeichnis enthält dann die Dateien, die die Laufzeitumgebung definieren (Befehle, Konfigurationsdateien, Protokolldateien usw.). Welches Verzeichnis standardmäßig verwendet wird, hängt von der Plattform ab:
    -   `installationsstammverz/profiles/  
profilname`
    -  `installationsstammverz\profiles\profilname`
 Dabei ist *profilname* der von Ihnen angegebene Name.  
 Das Feld für das Profilverzeichnis muss folgende Bedingungen erfüllen:
    - Der *profilname* muss eindeutig sein.
    - Das von Ihnen angegebene Verzeichnis muss leer sein.
    - Ihre Benutzer-ID muss für das Verzeichnis berechtigt sein.
    - Für die Erstellung des Profils muss ausreichend Speicherplatz vorhanden sein.
  - c) Optional: Sie können das Profil, das Sie erstellen, als Standardprofil definieren, sodass es von Befehlen automatisch verwendet wird. Wählen Sie hierzu das Kontrollkästchen **Dieses Profil als Standardprofil verwenden** aus. Dieses Kontrollkästchen wird nur angezeigt, wenn sich auf Ihrem System ein Profil befindet.  
 Beim Standardprofil funktionieren die Befehle automatisch. Das erste Profil, das Sie auf einer Workstation erstellen, ist das Standardprofil. Das Standardprofil ist das Standardziel für Befehle, die im Unterverzeichnis 'bin' des Installationsverzeichnisses eingegeben werden. Ist auf einer Workstation nur ein Profil vorhanden, dann wird jeder Befehl für dieses Profil ausgeführt. Bei Vorhandensein von mehr als einem Profil müssen Sie bei bestimmten Befehlen das Profil angeben, auf das sich der Befehl bezieht.
  - d) Klicken Sie auf **Weiter**.
- 2) Führen Sie auf der Seite mit den Namen für Knoten und Host die folgenden Aktionen für das Profil durch, das Sie erstellen:
  - a) Geben Sie im Feld 'Knotenname' einen Namen für den Knoten ein oder übernehmen Sie den Standardwert. Wählen Sie einen möglichst kurzen Knotennamen, aber stellen Sie sicher, dass jeder Knotenname in Ihrer Implementierungsumgebung eindeutig ist.
  - b) Geben Sie im Feld 'Hostname' einen Namen für den Host ein oder übernehmen Sie den Standardwert.
  - c) Geben Sie im Feld 'Zellenname' einen Namen für die Zelle ein oder übernehmen Sie den Standardwert.
 Klicken Sie auf **Weiter**, um die Seite 'Verwaltungssicherheit' anzuzeigen.

- 3) Auf der Seite 'Einbindung' können Sie auswählen, ob Sie den Knoten jetzt im Rahmen der Profilerstellung in den Deployment Manager einbinden oder ihn zu einem späteren Zeitpunkt und außerhalb der Profilerstellung mit dem Befehl `addNode` einbinden möchten. Wählen Sie das Kontrollkästchen **Diesen Knoten später einbinden** aus (bzw. inaktivieren Sie das Kontrollkästchen) und klicken Sie auf **Weiter**.
- 4) Geben Sie auf der Seite 'Sicherheitszertifikat (Teil 1)' an, ob Sie neue Zertifikate erstellen oder vorhandene Zertifikate importieren möchten. Führen Sie folgende Aktionen durch:
  - Um ein neues persönliches Standardzertifikat und ein neues Stammsignaturzertifikat zu erstellen, wählen Sie **Neues persönliches Standardzertifikat erstellen** und **Neues Stammsignaturzertifikat erstellen** aus und klicken Sie auf **Weiter**.
  - Um vorhandene Zertifikate zu importieren, wählen Sie **Vorhandenes persönliches Standardzertifikat importieren** und **Vorhandenes Stammsignaturzertifikat importieren** aus und geben Sie folgende Informationen an:
    - Geben Sie im Feld 'Pfad' den Verzeichnispfad zu dem vorhandenen Zertifikat ein.
    - Geben Sie im Feld 'Kennwort' das Kennwort für das Zertifikat ein.
    - Wählen Sie im Feld 'Keystore-Typ' den Keystore-Typ für das zu importierende Zertifikat aus.
    - Wählen Sie im Feld 'Keystore-Alias' das Keystore-Alias für das zu importierende Zertifikat aus.
    - Klicken Sie auf **Weiter**.

Wenn Sie ein persönliches Zertifikat als persönliches Standardzertifikat importieren, importieren Sie das Stammzertifikat, mit dem das persönliche Zertifikat signiert wurde. Andernfalls fügt das Profile Management Tool den Unterzeichner des persönlichen Zertifikats zur Datei `trust.p12` hinzu. Geben Sie beim Importieren des persönlichen Standardzertifikats oder des Stammsignaturzertifikats den Pfad und das Kennwort an und wählen Sie den Keystore-Typ und das Keystore-Alias für jedes Zertifikat aus, das Sie importieren.

- 5) Prüfen Sie auf der Seite 'Sicherheitszertifikat (Teil 1)', ob die Zertifikatsinformationen richtig sind, und klicken Sie auf **Weiter**, um die Seite für die Portwertzuordnung anzuzeigen.

Wenn Sie die Zertifikate erstellen, können Sie entweder die Standardwerte übernehmen oder die Werte für die Erstellung neuer Zertifikate ändern. Ein persönliches Standardzertifikat hat eine Standardgültigkeit von einem Jahr und wird vom Stammsignaturzertifikat signiert. Das Stammsignaturzertifikat ist ein selbst signiertes Zertifikat mit einer Standardgültigkeit von 15 Jahren. Das Keystore-Standardkennwort für das Stammsignaturzertifikat lautet `WebAS`. Ändern Sie dieses Kennwort. Das neue Kennwort darf keine Zeichen des Doppelbytezeichensatzes (DBCS) enthalten, da bestimmte Keystore-Typen, unter anderem auch `PKCS12`, diese Zeichen nicht unterstützen. Welche Keystore-Typen unterstützt werden, hängt von den Providern in der Datei `java.security` ab.

Wenn Sie ein oder beide Zertifikate erstellen oder ein oder beide Zertifikate importieren, werden die folgenden Keystore-Dateien erstellt:

- `key.p12`: Enthält das persönliche Standardzertifikat.
- `trust.p12`: Enthält das Unterzeichnerzertifikat vom Standardstammzertifikat.



- `root-key.p12`: Enthält das Stammsignaturzertifikat.
- `default-signers.p12`: Enthält Unterzeichnerzertifikate, die zu allen neuen Keystore-Dateien hinzugefügt werden, die Sie nach der Installation und Inbetriebnahme des Servers erstellt haben. Standardmäßig enthält die Keystore-Datei das Unterzeichnerzertifikat für das Standardstammzertifikat und ein DataPower-Unterzeichnerzertifikat.
- `deleted.p12`: Enthält Zertifikate, die mit der Task 'deleteKeyStore' gelöscht wurden und bei Bedarf wiederhergestellt werden können.
- `ltpa.jceks`: Enthält LTPA-Standardschlüssel (LTPA = Lightweight Third-Party Authentication) für Server, die die Server in Ihrer Umgebung verwenden, um miteinander zu kommunizieren.

Alle diese Dateien besitzen dasselbe Kennwort, wenn Sie die Zertifikate erstellen oder importieren. Hierbei handelt es sich entweder um das Standardkennwort oder um ein von Ihnen angegebenes Kennwort. Ein importiertes Zertifikat wird zur Datei `key.p12` oder zur Datei `root-key.p12` hinzugefügt. Wenn Sie Zertifikate importieren und diese Zertifikate nicht die gewünschten Informationen enthalten, klicken Sie auf **Zurück**, um ein anderes Zertifikat zu importieren.

- 6) Klicken Sie auf der Seite 'Profil - Zusammenfassung' auf die Option **Erstellen**, um das Profil zu erstellen, oder klicken Sie auf **Zurück**, um die Merkmale für das Profil zu ändern.

Der Fortschritt der Profilkonfiguration wird in einem eigenen Fenster angezeigt. Wenn die Profilerstellung abgeschlossen ist, wird eine Seite mit der Nachricht **Das Profile Management Tool hat das Profil erfolgreich erstellt.** angezeigt.

**Achtung:** Wenn Fehler bei der Profilerstellung festgestellt wurden, werden anstelle der Nachricht zur erfolgreichen Profilerstellung möglicherweise andere Nachrichten angezeigt, wie z. B.:

- **Das Profile Management Tool hat das Profil erstellt, wobei jedoch Fehler aufgetreten sind.** Diese Nachricht gibt an, dass die Profilerstellung zwar durchgeführt wurde, aber Fehler generiert wurden.
- **Das Profile Management Tool kann das Profil nicht erstellen.** Diese Nachricht gibt an, dass die Profilerstellung vollständig fehlgeschlagen ist.




Auf der Seite zur Fertigstellung des Profils wird zur Fehlerbehebung auf die Protokolldatei verwiesen.

4. Melden Sie sich bei der Deployment Manager-Administrationskonsole an.
5. Abhängig davon, ob Sie Business Space für einen Cluster oder für verwaltete Server implementieren wollen, führen Sie eine der folgenden Aktionen aus:
  - Für einen Cluster:
    - a. Erstellen Sie einen Cluster von Anwendungsservern.
    - b. Fügen Sie ein oder mehr Cluster-Member zu dem Cluster hinzu (dies sind die angepassten Profile (Business Space), die zuvor erstellt wurden).
  - Für jeden verwalteten Server:
    - a. Erstellen Sie einen Anwendungsserver.
    - b. Wählen Sie den Knoten des verwalteten Servers als das angepasste Profil (Business Space) aus, das zuvor erstellt wurde.
6. Stoppen Sie das Deployment Manager-Profil.

Stoppen Sie den Deployment Manager mithilfe des Befehls `stopServer` im Verzeichnis `profilstammverzeichnis/bin`.



Verwenden Sie die folgende Syntax:

-   `stopServer.sh servername -username benutzername -password kennwort`
-  `stopServer.bat servername -username benutzername -password kennwort`

Wenn die Sicherheit für das Profil nicht aktiviert ist, sind die Parameter `-username` und `-password` nicht erforderlich.

Weitere Informationen zum Befehl `stopServer` finden Sie im Abschnitt zum Befehl `stopServer` im Information Center von WebSphere Application Server Version 8.0.

7. Navigieren Sie zum Verzeichnis *installationsstammverzeichnis/BusinessSpace/config.bspace/MetadataFiles* und kopieren Sie - abhängig von dem Datenbanktyp, den Sie für Business Space verwenden werden - die relevante Datei in ein Arbeitsverzeichnis. Ändern Sie die Erweiterung dieser Datei nicht: Sie muss `.properties` lauten.
  - a. Bearbeiten Sie die Kopie dieser Datei und ändern Sie die Werte so, dass sie Ihrer Datenbank entsprechen. Stellen Sie sicher, dass die Eigenschaft `wasHome` korrekt ist.
  - b. Wenn Sie die Datei bearbeitet und auf Ihre Datenbankinformationen abgestimmt haben, speichern Sie die Datei.

Wenn Sie die Profile erstellt und die Datenbankinformationen für Ihre Profile konfiguriert haben, können Sie Business Space in Ihrer Umgebung konfigurieren, indem Sie folgende Schritte ausführen:

1. Führen Sie für jeden Cluster oder für jeden verwalteten Server den Befehl **installBusinessSpace** aus, um die EAR-Dateien für Business Space in der Laufzeitumgebung zu installieren. Geben Sie entweder den Parameter **clusterName** oder die Parameter **nodeName** und **serverName** an, abhängig davon, wie Sie Ihre Network Deployment-Topologie einrichten. Vgl. „Business Space über die Befehlszeile konfigurieren“ auf Seite 251.
2. Führen Sie für jeden Cluster oder verwalteten Server den Befehl **configureBusinessSpace** aus. Geben Sie dazu entweder den Parameter **clusterName** oder die Parameter **nodeName** und **serverName** an, abhängig davon, wie Sie Ihre Network Deployment-Topologie einrichten. Geben Sie außerdem den Parameter **bspacedbDesign** an. Der Wert für diesen Parameter sollte der Pfad zu der Datei mit den Datenbankeigenschaften sein, die Sie zuvor bearbeitet haben. Optional können Sie bei der Erstellung von Datenbanktabellen und der Konfiguration der Business Space-Datenbank den Parameter **createTables** als wahr (`true`) angeben. Vgl. „Business Space über die Befehlszeile konfigurieren“ auf Seite 251.
3. Speichern Sie die `wsadmin`-Konfiguration.
4. Wurde der Parameter **createTables** in Schritt 2 nicht vorgegeben, erstellen und konfigurieren Sie die Business Space-Datenbank. Vgl. „Business Space-Datenbank konfigurieren“ auf Seite 255.
5. Starten Sie den Deployment Manager.
6. Starten Sie die Cluster oder verwalteten Server.

*Business Space-Profil mithilfe des Befehlszeilendienstprogramms `manageprofiles` für eine Network Deployment-Konfiguration erstellen:*

Mit dem Befehlszeilendienstprogramm `manageprofiles` können Sie Deployment Manager-Profilen und angepasste Profile (verwaltete Knoten) für Ihre Business Space-Network Deployment-Konfiguration erstellen.

Stellen Sie vor der Ausführung des Befehlszeilendienstprogramms `manageprofiles` sicher, dass Sie die folgenden Tasks vollständig ausgeführt haben:

- Überprüfen Sie die vollständige Liste der Voraussetzungen für das Erstellen oder Erweitern eines Profils, die unter Profilkonzepte im Information Center von WebSphere Application Server aufgeführt ist.
- Schauen Sie sich die Beispiele mit Befehlen zur Profilerstellung an.
- Vergewissern Sie sich, dass das Befehlszeilendienstprogramm `manageprofiles` nicht bereits für dasselbe Profil ausgeführt wird. Wenn Sie eine Fehlermeldung erhalten, prüfen Sie, ob gleichzeitig noch eine weitere Profilerstellung oder Profilerweiterung durchgeführt wird. Wenn dies der Fall ist, müssen Sie auf den Abschluss dieser Erstellung bzw. Erweiterung warten.

Diese Task beschreibt, wie Sie mit dem Befehlszeilendienstprogramm `manageprofiles` Business Space-Profilen für Ihre Business Space-Network Deployment-Konfiguration erstellen können. Führen Sie die folgenden Schritte aus, um das Befehlszeilendienstprogramm `manageprofiles` zum Erstellen eines Profils zu verwenden.

1. Erstellen Sie das Deployment Manager-Profil.

- a. Lokalisieren Sie die Schablone `dmgr.bspace` für Business Space-Deployment Manager-Profilen, die Deployment Manager definieren. Ein Deployment Manager stellt eine Verwaltungsschnittstelle für eine logische Gruppe von Servern auf mindestens einer Workstation bereit.

Im Verzeichnis `installationsstammverzeichnis/profileTemplates/BusinessSpace` finden Sie Schablonen für die einzelnen Profile.

- b. Ermitteln Sie im Abschnitt „Befehlszeilendienstprogramm 'manageprofiles' (für Business Space-Profilen)“ auf Seite 224, welche Parameter für die Profilerstellung erforderlich sind. Ermitteln Sie die Werte, die Sie für das Profil angeben möchten. Überprüfen Sie hierzu die Standardwerte, um festzustellen, ob diese bedarfsgerecht für Ihr Profil sind. Beispielsweise können Sie die Parameter `-templatePath`, `-serverType`, `-enableAdminSecurity`, `-adminUserName` und `-adminPassword` aufnehmen.

- c. Führen Sie die Datei von der Befehlszeile aus. Im Folgenden finden Sie ein einfaches Beispiel:




```
manageProfiles -create -templatePath installationsstammverzeichnis/profileTemplates/BusinessSpace
-serverType DEPLOYMENT_MANAGER -enableAdminSecurity true -adminUserName administrator-ID -ad
```

Der Befehl zeigt bei seiner Ausführung den aktuellen Status an. Warten Sie, bis er beendet ist. Für die Datei gilt die normale Syntaxprüfung und die Datei wird wie jede andere Antwortdatei syntaktisch analysiert. Einzelwerte in der Antwortdatei werden als Befehlszeilenparameter behandelt.

2. Starten Sie das Deployment Manager-Profil.

Starten Sie den Deployment Manager mithilfe des Befehls `startServer` im Verzeichnis `profilstammverzeichnis/bin`.

Verwenden Sie die folgende Syntax:

-   `startServer.sh servername`
-  `startServer.bat servername`

Weitere Informationen zum Befehl `startServer` finden Sie im Abschnitt zum Befehl `startServer` im Information Center von WebSphere Application Server Version 8.0.

3. Erstellen Sie die angepassten (benutzerdefinierten) Profile (verwaltete Knoten).
  - a. Lokalisieren Sie die Schablone `managed.bspace` für angepasste Profile (Business Space), die bei Einbindung in einen Deployment Manager verwaltete Knoten definieren. Falls für Ihre Lösung eine Implementierungsumgebung erforderlich ist, benötigen Sie für Ihre Laufzeitumgebung mindestens einen verwalteten Knoten. Ein benutzerdefiniertes Profil enthält einen leeren Knoten, den Sie in eine Deployment Manager-Zelle einbinden müssen, damit dieser verwendet werden kann. Wenn Sie ein benutzerdefiniertes Profil einbinden, wird es zu einem verwalteten Knoten. Binden Sie einen Knoten nur ein, wenn der Deployment Manager, in den die Einbindung erfolgt, das gleiche oder ein höheres Release-Level als das benutzerdefinierte Profil aufweist, das von Ihnen erstellt wird.

Im Verzeichnis `installationsstammverzeichnis/profileTemplates/BusinessSpace` finden Sie Schablonen für die einzelnen Profile.




- b. Ermitteln Sie im Abschnitt „Befehlszeilendienstprogramm 'manageprofiles' (für Business Space-Profil)“ auf Seite 224, welche Parameter für die Profilerstellung erforderlich sind. Ermitteln Sie die Werte, die Sie für das Profil angeben möchten. Überprüfen Sie hierzu die Standardwerte, um festzustellen, ob diese bedarfsgerecht für Ihr Profil sind. Beispielsweise können Sie die Parameter `-templatePath`, `-dmgrAdminUserName`, `-dmgrAdminPassword`, `-dmgrPort` und `-dmgrHost` aufnehmen.
  - c. Führen Sie die Datei von der Befehlszeile aus. Im Folgenden finden Sie ein einfaches Beispiel:

```
manageProfiles -create -templatePath installationsstammverzeichnis/profileTemplates/BusinessSpace
-dmgrAdminUserName deployment_manager-administrator-ID -dmgrAdminPassword deployment_manager-administrator-password
-dmgrPort deployment_manager-port -dmgrHost deployment_manager-hostname
```

Der Befehl zeigt bei seiner Ausführung den aktuellen Status an. Warten Sie, bis er beendet ist. Für die Datei gilt die normale Syntaxprüfung und die Datei wird wie jede andere Antwortdatei syntaktisch analysiert. Einzelwerte in der Antwortdatei werden als Befehlszeilenparameter behandelt.

4. Melden Sie sich bei der Deployment Manager-Administrationskonsole an.
5. Abhängig davon, ob Sie Business Space für einen Cluster oder für verwaltete Server implementieren, erstellen Sie Folgendes:
  - Für einen Cluster:
    - a. Erstellen Sie einen Cluster von Anwendungsservern.
    - b. Fügen Sie ein oder mehr Cluster-Member zu dem Cluster hinzu (dies sind die angepassten Profile (Business Space), die zuvor erstellt wurden).
  - Für jeden verwalteten Server:
    - a. Erstellen Sie einen Anwendungsserver.
    - b. Wählen Sie den Knoten des verwalteten Servers als das angepasste Profil (Business Space) aus, das zuvor erstellt wurde.
6. Stoppen Sie das Deployment Manager-Profil.  
Stoppen Sie den Deployment Manager mithilfe des Befehls `stopServer` im Verzeichnis `profilstammverzeichnis/bin`.

Verwenden Sie die folgende Syntax:

-   `stopServer.sh servername -username benutzername -password kennwort`
-  `stopServer.bat servername -username benutzername -password kennwort`

Wenn die Sicherheit für das Profil nicht aktiviert ist, sind die Parameter `-username` und `-password` nicht erforderlich.

Weitere Informationen zum Befehl `stopServer` finden Sie im Abschnitt zum Befehl `stopServer` im Information Center von WebSphere Application Server Version 8.0.

7. Navigieren Sie zum Verzeichnis *installationsstammverzeichnis/* `BusinessSpace/config.bspace/MetadataFiles` und kopieren Sie - abhängig von dem Datenbanktyp, den Sie für Business Space verwenden werden - die relevante Datei in ein Arbeitsverzeichnis. Ändern Sie die Erweiterung dieser Datei nicht: Sie muss `.properties` lauten.
  - a. Bearbeiten Sie die Kopie dieser Datei und ändern Sie die Werte so, dass sie Ihrer Datenbank entsprechen. Achten Sie besonders auf die richtigen Einstellungen für die Eigenschaft `wasHome`.
  - b. Wenn Sie die Datei bearbeitet und auf Ihre Datenbankinformationen abgestimmt haben, speichern Sie die Datei.

Wenn Sie die Profile erstellt und die Datenbankinformationen für Ihre Profile konfiguriert haben, können Sie Business Space in Ihrer Umgebung konfigurieren, indem Sie folgende Schritte ausführen:

1. Führen Sie für jeden Cluster oder für jeden verwalteten Server den Befehl **`installBusinessSpace`** aus, um die EAR-Dateien für Business Space in der Laufzeitumgebung zu installieren. Geben Sie entweder den Parameter **`clusterName`** oder die Parameter **`nodeName`** und **`serverName`** an, abhängig davon, wie Sie Ihre Network Deployment-Topologie einrichten. Vgl. „Business Space über die Befehlszeile konfigurieren“ auf Seite 251.
2. Führen Sie für jeden Cluster oder verwalteten Server den Befehl **`configureBusinessSpace`** aus. Geben Sie dazu entweder den Parameter **`clusterName`** oder die Parameter **`nodeName`** und **`serverName`** an, abhängig davon, wie Sie Ihre Network Deployment-Topologie einrichten. Geben Sie außerdem den Parameter **`bspacedbDesign`** an. Der Wert für diesen Parameter sollte der Pfad zu der Datei mit den Datenbankeigenschaften sein, die Sie zuvor bearbeitet haben. Optional können Sie bei der Erstellung von Datenbanktabellen und der Konfiguration der Business Space-Datenbank den Parameter **`createTables`** als wahr (`true`) angeben. Vgl. „Business Space über die Befehlszeile konfigurieren“ auf Seite 251.
3. Speichern Sie die `wsadmin`-Konfiguration.
4. Wurde der Parameter **`createTables`** in Schritt 2 nicht vorgegeben, erstellen und konfigurieren Sie die Business Space-Datenbank. Vgl. „Business Space-Datenbank konfigurieren“ auf Seite 255.
5. Starten Sie den Deployment Manager.
6. Starten Sie die Cluster oder verwalteten Server.

*Business Space-Profil für eine eigenständige Konfiguration erweitern:*

Um Business Space-Profil für eine eigenständige Umgebung zu erweitern, können Sie entweder das Profile Management Tool oder das Befehlszeilendienstprogramm `manageprofiles` verwenden.

Wenn Business Space im Rahmen Ihres Produktprofils konfiguriert wird, sind diese Tasks optional.

*Business Space-Profil mithilfe von Profile Management Tool für eine eigenständige Konfiguration erweitern:*

Sie können das Profile Management Tool verwenden, um eigenständige Profile für Business Space zu erweitern.

In diesem Abschnitt erhalten Sie Informationen darüber, was Profile sind, einschließlich der Unterschiede zwischen eigenständigen, Network Deployment- und angepassten Profilen. Sie erhalten Informationen über die Unterschiede zwischen der Option 'Typische Profilerweiterung' und der Option 'Erweiterte Profilerweiterung' - mit Hinweisen dazu, in welchen Szenarien die eine und welche die andere verwendet werden sollte. Bei der Option 'Typische Profilerweiterung' wird ein Profil mit Standardkonfigurationseinstellungen erweitert. Bei der Option 'Erweiterte Profilerweiterung' können Sie Ihre eigenen Konfigurationswerte für das Profil angeben, das Sie erweitern.




- Überprüfen Sie die vollständige Liste der Voraussetzungen für das Erstellen oder Erweitern eines Profils, die unter Profilkonzepte im Information Center von WebSphere Application Server aufgeführt ist.
- Wenn Sie das Profile Management Tool mit der grafischen Benutzerschnittstelle Motif auf einem Solaris-Betriebssystem verwenden, kann es vorkommen, dass die Standardgröße des Profile Management Tools zu klein ist, um alle Nachrichten und Schaltflächen des Profile Management Tools anzuzeigen.
- Wenn Sie beabsichtigen, eine Datenbankentwurfsdatei für die Business Space-Datenbankinformationen zu verwenden, führen Sie die Schritte in „Eigenschaftendatei für Business Space-Datenbankentwurf erstellen“ auf Seite 254 aus.

Mit diesem Verfahren können Sie ein Business Space-Profil für eine eigenständige Konfiguration erweitern. Die Schritte beschreiben die Profilerstellungsoptionen 'Erweiterte Profilerstellung' und 'Typische Profilerstellung'.

Wenn Business Space im Rahmen Ihres Produktprofils erweitert wird, ist diese Task optional.

1. Starten Sie das Profile Management Tool.

Verwenden Sie einen der folgenden Befehle:

-   `installationsstammverz/bin/ProfileManagement/pmt.sh`
-  `installationsstammverz\bin\ProfileManagement\pmt.bat`

Die Seite 'Willkommen' wird angezeigt.

2. Klicken Sie auf der Seite 'Willkommen' auf die Schaltfläche **Profile Management Tool starten** oder auf die Registerkarte 'Profile Management Tool'.

Die Registerkarte 'Profile' wird angezeigt.

In der Registerkarte 'Profile' wird eine Liste der Profile angezeigt, die sich zu diesem Zeitpunkt auf der Maschine befinden. Bei dem hier beschriebenen Verfahren wird davon ausgegangen, dass Sie ein vorhandenes Anwendungsserverprofil mit Business Space in einer eigenständigen Konfiguration erweitern.

3. Wählen Sie das Profil aus, das Sie erweitern wollen, und klicken Sie auf **Erweitern**. Die Schaltfläche **Erweitern** kann nur ausgewählt werden, wenn ein Profil erweitert werden kann.

Die Seite 'Erweiterungsauswahl' wird in einem separaten Fenster geöffnet.

4. Wenn das betreffende Profil auf Business Space erweitert werden kann, steht die Option **Eigenständiges Profil** auf der Seite 'Erweiterungsauswahl' zur Verfügung. Klicken Sie auf **Weiter**.
5. Entscheiden Sie auf der Seite 'Profilerweiterungsoptionen', ob das eigenständige Profil mithilfe der Option **Typische Profilerweiterung** oder **Erweiterte Profilerweiterung** erweitert werden soll.

Bei der Option 'Typische Profilerweiterung' wird ein Profil mit Standardkonfigurationseinstellungen erweitert. Bei der Option 'Erweiterte Profilerweiterung' können Sie Ihre eigenen Konfigurationswerte für das Profil angeben, das Sie erweitern.

6. Wenn Sie die Option **Typische Profilerweiterung** gewählt haben, führen Sie folgende Schritte aus:
  - a. Geben Sie auf der Seite 'Verwaltungssicherheit' nochmals die Benutzer-ID mit Administratorberechtigung und das zugehörige Kennwort für das Profil ein, das Sie erweitern wollen.
  - b. Klicken Sie auf der Seite 'Profilerweiterung - Zusammenfassung' auf die Option **Erweitern**, um das Profil zu erweitern, oder klicken Sie auf **Zurück**, um die Merkmale für das Profil zu ändern.

Der Fortschritt der Profilerweiterung wird in einem eigenen Fenster angezeigt. Wenn die Profilerweiterung abgeschlossen ist, wird eine Seite zur Fertigstellung der Profilerweiterung mit der Nachricht **Das Profile Management Tool hat das Profil erfolgreich erweitert.** angezeigt.

**Achtung:** Wenn Fehler bei der Profilerweiterung festgestellt werden, werden anstelle der Nachricht zur erfolgreichen Profilerweiterung möglicherweise andere Nachrichten angezeigt, wie z. B.:

- **Das Profile Management Tool hat das Profil erweitert, wobei jedoch Fehler aufgetreten sind.** Diese Nachricht gibt an, dass die Profilerweiterung zwar durchgeführt wurde, aber Fehler generiert wurden.
- **Das Profile Management Tool kann das Profil nicht erweitern.** Diese Nachricht gibt an, dass die Profilerweiterung vollständig fehlgeschlagen ist.

Auf der Seite zur Fertigstellung der Profilerweiterung wird zur Fehlerbehebung auf die Protokolldatei verwiesen.

7. Wenn Sie die Option **Erweiterte Profilerweiterung** gewählt haben, führen Sie folgende Schritte aus:
  - a. Geben Sie auf der Seite 'Verwaltungssicherheit' nochmals die Benutzer-ID mit Administratorberechtigung und das zugehörige Kennwort für das Profil ein, das Sie erweitern wollen.
  - b. Wenn Sie eine Entwurfsdatei verwenden wollen, die Sie bereits erstellt haben, um die Datenbanken für das erweiterte Profil zu konfigurieren, führen Sie die folgenden Schritte aus, anstatt die Datenbankkonfigurationseiten zu verwenden.
    - 1) Wählen Sie **Datenbankentwurfsdatei verwenden** für die Datenbankkonfiguration aus.
    - 2) Klicken Sie auf **Durchsuchen**.
    - 3) Geben Sie den vollständig qualifizierten Pfadnamen für die Entwurfsdatei an.
    - 4) Klicken Sie auf **Weiter**.
  - c. Wenn Sie keine Datenbankentwurfsdatei verwendet haben, führen Sie auf der Seite 'Datenbankkonfiguration' folgende Aktionen durch:
    - 1) Wählen Sie aus der Liste 'Datenbankprodukt auswählen' das Datenbankprodukt aus, das von dem Profil verwendet werden soll.
    - 2) Wählen Sie das Kontrollkästchen **Standardausgabeverzeichnis für Datenbankscripts außer Kraft setzen** aus, wenn Sie das Verzeichnis festlegen wollen, in das die SQL-Scripts zur Erstellung der Datenbanktabellen



geschrieben werden. Wenn Sie das Kontrollkästchen nicht auswählen, werden die Scripts in das Standardverzeichnis ausgegeben.

- 3) Klicken Sie auf **Weiter**, um die Seite 'Datenbankkonfiguration (Teil 2)' anzuzeigen.

Die auf der Seite 'Datenbankkonfiguration (Teil 2)' angezeigten Informationen hängen von dem Wert ab, der in der Liste 'Datenbankprodukt auswählen' auf der Seite 'Datenbankkonfiguration' angegeben wurde.

- d. Führen Sie die Datenbankkonfiguration auf der Seite 'Datenbankkonfiguration (Teil 2)' durch. Abhängig von Ihrem Datenbankprodukt müssen Sie eventuell einen Benutzernamen und ein Kennwort zur Authentifizierung bei der Datenbank sowie die JDBC-Treiberinformationen, Host, Port und Schema angeben.
- e. Klicken Sie auf der Seite 'Profilerweiterung - Zusammenfassung' auf die Option **Erweitern**, um das Profil zu erweitern, oder klicken Sie auf **Zurück**, um die Merkmale für das Profil zu ändern.

Der Fortschritt der Profilerweiterung wird in einem eigenen Fenster angezeigt. Wenn die Profilerweiterung abgeschlossen ist, wird eine Seite zur Fertigstellung der Profilerweiterung mit der Nachricht **Das Profile Management Tool hat das Profil erfolgreich erweitert.** angezeigt.

**Achtung:** Wenn Fehler bei der Profilerweiterung festgestellt werden, werden anstelle der Nachricht zur erfolgreichen Profilerweiterung möglicherweise andere Nachrichten angezeigt, wie z. B.:

- **Das Profile Management Tool hat das Profil erweitert, wobei jedoch Fehler aufgetreten sind.** Diese Nachricht gibt an, dass die Profilerweiterung zwar durchgeführt wurde, aber Fehler generiert wurden.
- **Das Profile Management Tool kann das Profil nicht erweitern.** Diese Nachricht gibt an, dass die Profilerweiterung vollständig fehlgeschlagen ist.

Auf der Seite zur Fertigstellung der Profilerweiterung wird zur Fehlerbehebung auf die Protokolldatei verwiesen.

Wenn Sie ein Profil erweitern, für das die Sicherheit bereits mit einem Benutzerrepository eingerichtet wurde (und zwar nicht die Standardoption für eingebundene Repositories), müssen Sie in der Datei `ConfigServices.properties` prüfen, ob der Parameter `MashupAdminForOOBspace` angepasst werden muss. Vgl. „Benutzerrepository für Business Space auswählen“ auf Seite 282.

*Business Space-Profil mithilfe des Befehlszeilendienstprogramms `manageprofiles` für eine eigenständige Konfiguration erweitern:*

Sie können eigenständige Profile für Business Space über die Befehlszeile erweitern, indem Sie das Befehlszeilendienstprogramm `manageprofiles` verwenden.

Stellen Sie vor der Ausführung des Befehlszeilendienstprogramms **`manageprofiles`** zum Erweitern eines Profils sicher, dass Sie die folgenden Tasks vollständig ausgeführt haben:

- Überprüfen Sie die vollständige Liste der Voraussetzungen für das Erstellen oder Erweitern eines Profils, die unter Profilkonzepte im Information Center von WebSphere Application Server aufgeführt ist.
- Schauen Sie sich die Beispiele mit Befehlen zur Profilerstellung an.
- Vergewissern Sie sich, das Befehlszeilendienstprogramm `manageprofiles` nicht bereits für dasselbe Profil ausgeführt wird. Wenn Sie eine Fehlernachricht erhalten

ten, prüfen Sie, ob gleichzeitig noch eine weitere Profilerstellung oder Profilerweiterung durchgeführt wird. Wenn dies der Fall ist, müssen Sie auf den Abschluss dieser Erstellung bzw. Erweiterung warten.

- Fahren Sie alle Server herunter, die in Beziehung zu dem Profil stehen, das erweitert werden soll.
- Ermitteln Sie, ob das Profil, das Sie erweitern möchten, bereits in einen Deployment Manager eingebunden wurde. Falls das Profil, das Sie erweitern möchten, bereits in einen Deployment Manager eingebunden wurde, können Sie es nicht mit dem Befehlszeilendienstprogramm `manageprofiles` erweitern.
- Bestimmen Sie, mit welcher Schablone das vorhandene Profil erstellt wurde (Deployment Manager, eigenständig oder verwaltet). Sie können die für die Erstellung des Profils verwendete Schablone feststellen, indem Sie die Daten in der Profilregistry prüfen, die sich im Verzeichnis `installationsstammverzeichnis/properties/profileRegistry.xml` befindet. Ändern Sie diese Datei nicht, sondern verwenden Sie sie nur, um die Schablonen anzuzeigen. Bei dieser Prozedur wird davon ausgegangen, dass Sie ein eigenständiges Process Server-Profil erweitern.

Führen Sie die folgenden Schritte aus, um mit dem Befehlszeilendienstprogramm **manageprofiles** ein Business Space-Profil für eine eigenständige Konfiguration zu erweitern.

Wenn Business Space im Rahmen Ihres Produktprofils erweitert wird, ist diese Task optional.

1. Lokalisieren Sie die Profilschablone `default.bspace` für eigenständige Profile (Business Space), die eigenständige Server definieren.

Im Verzeichnis `installationsstammverzeichnis/profileTemplates/BusinessSpace` finden Sie Schablonen für die einzelnen Profile.

Sie verwenden den Parameter **augment**, um mit einer Erweiterungsschablone Änderungen an einem vorhandenen Profil durchzuführen. Der Parameter **augment** bewirkt, dass das Befehlszeilendienstprogramm **manageprofiles** das im Parameter **-profileName** angegebene Profil anhand der Schablone aktualisiert oder erweitert, die im Parameter **-templatePath** angegeben ist. Die Erweiterungsschablonen, die Sie verwenden können, sind von den IBM Produkten und den Versionen abhängig, die in Ihrer Umgebung installiert sind. Vergewissern Sie sich, dass Sie den vollständig qualifizierten Dateipfad für **-templatePath** angegeben haben, da ein relativer Dateipfad dazu führt, dass das angegebene Profil nicht vollständig erweitert werden kann.

2. Führen Sie die Datei von der Befehlszeile aus. Geben Sie den Parameter **-profilePath** nicht an. Im Folgenden finden Sie ein einfaches Beispiel:

```
manageProfiles -augment -profileName profilname -templatePath
installationsstammverzeichnis/profileTemplates/BusinessSpace/default.bspace -cellName zellename
-nodeName knotenname -enableAdminSecurity true -adminUserName admin
-adminPassword admin -dbType DB2_Universal -dbUserId datenbankbenutzer-ID
-dbPassword datenbankkennwort -dbJDBCClasspath installationsstammverzeichnis/jdbcdrivers/DB2
-dbName datenbankname -bspaceSchema datenbankschema -dbHostName
datenbank-hostname -dbServerPort datenbankport -dbDelayConfig false
```

Die Angabe der Parameter **-cellName** und **-nodeName** ist optional. Wenn Sie die beiden Parameter **-cellName** und **-nodeName** nicht festlegen, wird standardmäßig das von Ihnen verwendete, vorhandene Profil ausgewählt.

Der Status wird im Konsolfenster ausgegeben, wenn die Befehlsausführung abgeschlossen ist.

Wenn Sie ein Profil erweitern, für das die Sicherheit bereits mit einem Benutzerrepository eingerichtet wurde (und zwar nicht die Standardoption für eingebundene Repositories), müssen Sie in der Datei `ConfigServices.properties` prüfen, ob der

Parameter MashupAdminForOOBSpace angepasst werden muss. Vgl. „Benutzerrepositorium für Business Space auswählen“ auf Seite 282.

*Business Space-Profil für eine Network Deployment-Konfiguration erweitern:*

Um Business Space-Profil für eine Network Deployment-Konfiguration zu erweitern, können Sie entweder das Profile Management Tool oder das Befehlszeilendienstprogramm manageprofiles verwenden.

Wenn Business Space im Rahmen Ihres Produktprofils konfiguriert wird, sind diese Tasks optional.

*Business Space-Profil mithilfe des Profile Management Tool für eine Network Deployment-Konfiguration erweitern:*

Sie können das Profile Management Tool verwenden, um Business Space-Profil für eine Network Deployment-Umgebung zu erweitern.

In diesem Abschnitt erhalten Sie Informationen darüber, was Profile sind, einschließlich der Unterschiede zwischen eigenständigen, Network Deployment- und angepassten Profilen. Sie erhalten Informationen über die Unterschiede zwischen der Option 'Typische Profilerweiterung' und der Option 'Erweiterte Profilerweiterung' - mit Hinweisen dazu, in welchen Szenarien die eine und welche die andere verwendet werden sollte. Bei der Option 'Typische Profilerweiterung' wird ein Profil mit Standardkonfigurationseinstellungen erweitert. Bei der Option 'Erweiterte Profilerweiterung' können Sie Ihre eigenen Konfigurationswerte für das Profil angeben, das Sie erweitern.

- Überprüfen Sie die vollständige Liste der Voraussetzungen für das Erstellen oder Erweitern eines Profils, die unter Profilkonzepte im Information Center von WebSphere Application Server aufgeführt ist.
- Wenn Sie das Profile Management Tool mit der grafischen Benutzerschnittstelle Motif auf einem Solaris-Betriebssystem verwenden, kann es vorkommen, dass die Standardgröße des Profile Management Tool zu klein ist, um alle Nachrichten und Schaltflächen des Profile Management Tool anzuzeigen.




Mit diesem Verfahren können Sie ein Business Space-Profil für eine Network Deployment-Konfiguration erweitern. Die Schritte beschreiben die Profilerweiterungsoptionen 'Erweiterte Profilerstellung' und 'Typische Profilerstellung'. Die Prozedur setzt voraus, dass ein Deployment Manager-Profil und angepasste Profile (verwaltete Knoten) vorhanden sind, die Sie für Business Space erweitern möchten.

Wenn Business Space im Rahmen Ihres Produktprofils erweitert wird, ist diese Task optional.

1. Erweitern Sie das Deployment Manager-Profil.

a. Starten Sie das Profile Management Tool.

Verwenden Sie einen der folgenden Befehle:

-   `installationsstammverz/bin/ProfileManagement/pmt.sh`
-  `installationsstammverz\bin\ProfileManagement\pmt.bat`

b. Klicken Sie auf der Seite 'Willkommen' auf die Schaltfläche **Profile Management Tool starten** oder auf die Registerkarte 'Profile Management Tool'.

Die Registerkarte 'Profile' wird angezeigt.

In der Registerkarte 'Profile' wird eine Liste der Profile angezeigt, die auf der Maschine erstellt wurden. Sie können das Profile Management Tool verwenden, um neue Profile zu erstellen oder vorhandene Profile zu erweitern.

- c. Klicken Sie in der Registerkarte 'Profile' auf die Schaltfläche **Erweitern**. Die Seite 'Erweiterungsauswahl' wird in einem separaten Fenster geöffnet.
- d. Erweitern Sie auf der Seite 'Erweiterungsauswahl' den Abschnitt **Business Space powered by WebSphere**, wählen Sie die Option **Business Space-Deployment Manager** und klicken Sie auf **Weiter**.
- e. Entscheiden Sie auf der Seite 'Profilerweiterungsoptionen', ob das eigenständige Profil mithilfe der Option **Typische Profilerweiterung** oder **Erweiterte Profilerweiterung** erweitert werden soll.
- f. Geben Sie auf der Seite 'Verwaltungssicherheit' Werte für Benutzernamen und Kennwort ein, bestätigen Sie das Kennwort und klicken Sie auf **Weiter**. Alle Profileinstellungen, einschließlich Profilooptionen, werden standardmäßig konfiguriert und auf der Seite 'Profilerweiterung - Zusammenfassung' angezeigt.
- g. Klicken Sie auf der Seite 'Profilerweiterung - Zusammenfassung' auf die Option **Erweitern**, um das Profil zu erweitern, oder klicken Sie auf **Zurück**, um die Merkmale für das Profil zu ändern.

Der Fortschritt der Profilkonfiguration wird in einem eigenen Fenster angezeigt. Wenn die Profilerstellung abgeschlossen ist, wird eine Seite zur Fertigstellung der Profilerweiterung mit der Nachricht **Das Profile Management Tool hat das Profil erfolgreich erweitert** angezeigt.

**Achtung:** Wenn Fehler bei der Profilerweiterung festgestellt werden, werden anstelle der Nachricht zur erfolgreichen Profilerweiterung möglicherweise andere Nachrichten angezeigt, wie z. B.:



- **Das Profile Management Tool hat das Profil erweitert, wobei jedoch Fehler aufgetreten sind.** Diese Nachricht gibt an, dass die Profilerweiterung zwar durchgeführt wurde, aber Fehler generiert wurden.
- **Das Profile Management Tool kann das Profil nicht erweitern.** Diese Nachricht gibt an, dass die Profilerweiterung vollständig fehlgeschlagen ist.

Auf der Seite zur Fertigstellung der Profilerweiterung wird zur Fehlerbehebung auf die Protokolldatei verwiesen.

## 2. Starten Sie das Profil.

Starten Sie das Profil mithilfe des Befehls `startServer` im Verzeichnis `profilstammverzeichnis/bin`.

Verwenden Sie die folgende Syntax:



-  `startServer.sh servername`
-  `startServer.bat servername`


Weitere Informationen zum Befehl `startServer` finden Sie im Abschnitt zum Befehl `startServer` im Information Center von WebSphere Application Server Version 8.0.

## 3. Erweitern Sie die angepassten (benutzerdefinierten) Profile (verwaltete Knoten).

### a. Starten Sie das Profile Management Tool.

Verwenden Sie einen der folgenden Befehle:

-   `installationsstammverz/bin/ProfileManagement/pmt.sh`

-  `installationsstammverz\bin\ProfileManagement\pmt.bat`
- b. Klicken Sie auf der Seite 'Willkommen' auf die Schaltfläche **Profile Management Tool starten** oder auf die Registerkarte 'Profile Management Tool'.  
Die Registerkarte 'Profile' wird angezeigt.  
In der Registerkarte 'Profile' wird eine Liste der Profile angezeigt, die auf der Maschine erstellt wurden. Sie können das Profile Management Tool verwenden, um neue Profile zu erstellen oder vorhandene Profile zu erweitern.
  - c. Klicken Sie in der Registerkarte 'Profile' auf die Schaltfläche **Erweitern**.  
Die Seite 'Erweiterungsauswahl' wird in einem separaten Fenster geöffnet.
  - d. Erweitern Sie auf der Seite 'Erweiterungsauswahl' den Abschnitt **Business Space powered by WebSphere**, wählen Sie die Option **Angepasstes Profil (Business Space)** und klicken Sie auf **Weiter**.
  - e. Entscheiden Sie auf der Seite 'Profileroptionsmöglichkeiten', ob das eigenständige Profil mithilfe der Option **Typische Profilerstellung** oder **Erweiterte Profilerstellung** erstellt werden soll.
  - f. Auf der Seite 'Einbindung' können Sie auswählen, ob Sie den Knoten jetzt im Rahmen der Profilerstellung in den Deployment Manager einbinden oder ihn zu einem späteren Zeitpunkt und außerhalb der Profilerstellung mit dem Befehl `addNode` einbinden möchten. Wählen Sie das Kontrollkästchen **Diesen Knoten später einbinden** aus (bzw. inaktivieren Sie das Kontrollkästchen) und klicken Sie auf **Weiter**.
  - g. Klicken Sie auf der Seite 'Profileroptionsmöglichkeiten - Zusammenfassung' auf die Option **Erstellen**, um das Profil zu erstellen, oder klicken Sie auf **Zurück**, um die Merkmale für das Profil zu ändern.

Der Fortschritt der Profilkonfiguration wird in einem eigenen Fenster angezeigt. Wenn die Profilerstellung abgeschlossen ist, wird eine Seite zur Fertigstellung der Profilerweiterung mit der Nachricht **Das Profile Management Tool hat das Profil erfolgreich erweitert** angezeigt.

**Achtung:** Wenn Fehler bei der Profilerstellung festgestellt wurden, werden anstelle der Nachricht zur erfolgreichen Profilerstellung möglicherweise andere Nachrichten angezeigt, wie z. B.:

- **Das Profile Management Tool hat das Profil erweitert, wobei jedoch Fehler aufgetreten sind.** Diese Nachricht gibt an, dass die Profilerstellung zwar durchgeführt wurde, aber Fehler generiert wurden.
- **Das Profile Management Tool kann das Profil nicht erweitern.** Diese Nachricht gibt an, dass die Profilerstellung vollständig fehlgeschlagen ist.

Auf der Seite zur Fertigstellung der Profilerweiterung wird zur Fehlerbehebung auf die Protokolldatei verwiesen.




4. Melden Sie sich bei der Deployment Manager-Administrationskonsole an.
5. Optional: Wenn Sie noch über einen Cluster oder verwaltete Server verfügen, führen Sie eine der folgenden Aktionen für Ihre Umgebung aus:
  - Für einen Cluster:
    - a. Erstellen Sie einen Cluster von Anwendungsservern.
    - b. Fügen Sie ein oder mehr Cluster-Member zu dem Cluster hinzu (dies sind die angepassten Profile (Business Space), die zuvor erstellt wurden).
  - Für jeden verwalteten Server:
    - a. Erstellen Sie einen Anwendungsserver.
    - b. Wählen Sie den Knoten des verwalteten Servers als das angepasste Profil (Business Space) aus, das zuvor erstellt wurde.



6. Stoppen Sie das Deployment Manager-Profil.

Stoppen Sie den Deployment Manager mithilfe des Befehls `stopServer` im Verzeichnis `profilstammverzeichnis/bin`.

Verwenden Sie die folgende Syntax:

-   `stopServer.sh servername -username benutzername -password kennwort`
-  `stopServer.bat servername -username benutzername -password kennwort`

Wenn die Sicherheit für das Profil nicht aktiviert ist, sind die Parameter `-username` und `-password` nicht erforderlich.

Weitere Informationen zum Befehl `stopServer` finden Sie im Abschnitt zum Befehl `stopServer` im Information Center von WebSphere Application Server Version 8.0.

7. Navigieren Sie zum Verzeichnis `installationsstammverzeichnis/`

`BusinessSpace/config.bspace/MetadataFiles` und kopieren Sie - abhängig von dem Datenbanktyp, den Sie für Business Space verwenden werden - die relevante Datei in ein Arbeitsverzeichnis. Ändern Sie die Erweiterung dieser Datei nicht: Sie muss `.properties` lauten.

- a. Bearbeiten Sie die Kopie dieser Datei und ändern Sie die Werte so, dass sie Ihrer Datenbank entsprechen. Achten Sie besonders auf die richtigen Einstellungen für die Eigenschaft `wasHome`.
- b. Wenn Sie die Datei bearbeitet und auf Ihre Datenbankinformationen abgestimmt haben, speichern Sie die Datei.

Wenn Sie die Profile erstellt und die Datenbankinformationen für Ihre Profile konfiguriert haben, können Sie Business Space in Ihrer Umgebung konfigurieren, indem Sie folgende Schritte ausführen:

1. Führen Sie für jeden Cluster oder für jeden verwalteten Server den Befehl **`installBusinessSpace`** aus, um die EAR-Dateien für Business Space in der Laufzeitumgebung zu installieren. Geben Sie entweder den Parameter **`clusterName`** oder die Parameter **`nodeName`** und **`serverName`** an, abhängig davon, wie Sie Ihre Network Deployment-Topologie einrichten. Vgl. „Business Space über die Befehlszeile konfigurieren“ auf Seite 251.
2. Führen Sie für jeden Cluster oder verwalteten Server den Befehl **`configureBusinessSpace`** aus. Geben Sie dazu entweder den Parameter **`clusterName`** oder die Parameter **`nodeName`** und **`serverName`** an, abhängig davon, wie Sie Ihre Network Deployment-Topologie einrichten. Geben Sie außerdem den Parameter **`bspacedbDesign`** an. Der Wert für diesen Parameter sollte der Pfad zu der Datei mit den Datenbankeigenschaften sein, die Sie zuvor bearbeitet haben. Optional können Sie bei der Erstellung von Datenbanktabellen und der Konfiguration der Business Space-Datenbank den Parameter **`createTables`** als wahr (`true`) angeben. Vgl. „Business Space über die Befehlszeile konfigurieren“ auf Seite 251.
3. Speichern Sie die `wsadmin`-Konfiguration.
4. Wurde der Parameter **`createTables`** in Schritt 2 nicht vorgegeben, erstellen und konfigurieren Sie die Business Space-Datenbank. Vgl. „Business Space-Datenbank konfigurieren“ auf Seite 255.
5. Starten Sie den Deployment Manager.
6. Starten Sie die Cluster oder verwalteten Server.



Wenn Sie ein Profil erweitern, für das die Sicherheit bereits mit einem Benutzerrepository einrichtet wurde (und zwar nicht die Standardoption für eingebundene Repositories), müssen Sie in der Datei `ConfigServices.properties` prüfen, ob der Parameter `MashupAdminForOOBSpace` angepasst werden muss. Vgl. „Benutzerrepository für Business Space auswählen“ auf Seite 282.

*Business Space-Profil mithilfe des Befehlszeilendienstprogramms `manageprofiles` für eine Network Deployment-Konfiguration erweitern:*

Sie können Business Space-Profil für eine Network Deployment-Konfiguration über die Befehlszeile erweitern, indem Sie das Befehlszeilendienstprogramm `manageprofiles` verwenden.

Stellen Sie vor der Ausführung des Befehlszeilendienstprogramms **manageprofiles** zum Erweitern eines Profils sicher, dass Sie die folgenden Tasks vollständig ausgeführt haben:

- Überprüfen Sie die vollständige Liste der Voraussetzungen für das Erstellen oder Erweitern eines Profils, die unter Profilkonzepte im Information Center von WebSphere Application Server aufgeführt ist.
- Schauen Sie sich die Beispiele mit Befehlen zur Profilerstellung an.
- Vergewissern Sie sich, dass das Befehlszeilendienstprogramm `manageprofiles` nicht bereits für dasselbe Profil ausgeführt wird. Wenn Sie eine Fehlermeldung erhalten, prüfen Sie, ob gleichzeitig noch eine weitere Profilerstellung oder Profilerweiterung durchgeführt wird. Wenn dies der Fall ist, müssen Sie auf den Abschluss dieser Erstellung bzw. Erweiterung warten.
- Fahren Sie alle Server herunter, die in Beziehung zu dem Profil stehen, das erweitert werden soll.
- Ermitteln Sie, ob das Profil, das Sie erweitern möchten, bereits in einen Deployment Manager eingebunden wurde. Falls das Profil, das Sie erweitern möchten, bereits in einen Deployment Manager eingebunden wurde, können Sie es nicht mit dem Befehlszeilendienstprogramm `manageprofiles` erweitern.
- Bestimmen Sie, mit welcher Schablone das vorhandene Profil erstellt wurde (Deployment Manager, eigenständig oder verwaltet). Sie können die für die Erstellung des Profils verwendete Schablone feststellen, indem Sie die Daten in der Profilregistry prüfen, die sich im Verzeichnis `installationsstammverzeichnis/properties/profileRegistry.xml` befindet. Ändern Sie diese Datei nicht, sondern verwenden Sie sie nur, um die Schablonen anzuzeigen. Bei dieser Prozedur wird davon ausgegangen, dass Sie ein 'Business Space powered by WebSphere'-Deployment Manager-Profil erweitern.

Führen Sie die folgenden Schritte aus, um mit dem Befehlszeilendienstprogramm **manageprofiles** ein Business Space-Profil für eine Network Deployment-Konfiguration zu erweitern. Die Prozedur setzt voraus, dass ein Deployment Manager-Profil und angepasste Profile (verwaltete Knoten) vorhanden sind, die Sie für Business Space erweitern möchten.

Wenn Business Space im Rahmen Ihres Produktprofils erweitert wird, ist diese Task optional.

1. Erweitern Sie das Deployment Manager-Profil.
  - a. Lokalisieren Sie die Schablone `dmgr.bspace` für Business Space-Deployment Manager-Profil, die Deployment Manager definieren. Ein Deployment Manager stellt eine Verwaltungsschnittstelle für eine logische Gruppe von Servern auf mindestens einer Workstation bereit.

Im Verzeichnis *installationsstammverzeichnis/profileTemplates/BusinessSpace* finden Sie Schablonen für die einzelnen Profile.

- b. Ermitteln Sie im Abschnitt „Befehlszeilendienstprogramm 'manageprofiles' (für Business Space-Profile)“ auf Seite 224, welche Parameter für die Profilerweiterung erforderlich sind. Ermitteln Sie die Werte, die Sie für das Profil angeben möchten. Überprüfen Sie hierzu die Standardwerte, um festzustellen, ob diese bedarfsgerecht für Ihr Profil sind.

Sie verwenden den Parameter **augment**, um mit einer Erweiterungsschablone Änderungen an einem vorhandenen Profil durchzuführen. Der Parameter **augment** bewirkt, dass das Befehlszeilendienstprogramm **manageprofiles** das im Parameter **-profileName** angegebene Profil anhand der Schablone aktualisiert oder erweitert, die im Parameter **-templatePath** angegeben ist. Die Erweiterungsschablonen, die Sie verwenden können, sind von den IBM Produkten und den Versionen abhängig, die in Ihrer Umgebung installiert sind. Vergewissern Sie sich, dass Sie den vollständig qualifizierten Dateipfad für **-templatePath** angegeben haben, da ein relativer Dateipfad dazu führt, dass das angegebene Profil nicht vollständig erweitert werden kann.

- c. Führen Sie die Datei von der Befehlszeile aus. Im Folgenden finden Sie ein einfaches Beispiel:




```
manageProfiles -augment -profileName profilname
               -templatePath installationsstammverzeichnis/profileTemplates/BusinessSpace/dmgr.bspace
               -serverType DEPLOYMENT_MANAGER -cellName verwaltungszellename
               -nodeName verwaltungsknotename -enableAdminSecurity true
               -adminUserName administratorname -adminPassword administratorkennwort
```

Der Befehl zeigt bei seiner Ausführung den aktuellen Status an. Warten Sie, bis er beendet ist.

2. Starten Sie das Deployment Manager-Profil.

Starten Sie das Profil mithilfe des Befehls `startServer` im Verzeichnis *profilstammverzeichnis/bin*.

Verwenden Sie die folgende Syntax:

-   `startServer.sh servername`
-  `startServer.bat servername`

Weitere Informationen zum Befehl `startServer` finden Sie im Abschnitt zum Befehl `startServer` im Information Center von WebSphere Application Server Version 8.0.

3. Erweitern Sie die angepassten (benutzerdefinierten) Profile (verwaltete Knoten).

- a. Lokalisieren Sie die Schablone `managed.bspace` für angepasste Profile (Business Space), die bei Einbindung in einen Deployment Manager verwaltete Knoten definieren. Falls für Ihre Lösung eine Implementierungsumgebung erforderlich ist, benötigen Sie für Ihre Laufzeitumgebung mindestens einen verwalteten Knoten. Ein benutzerdefiniertes Profil enthält einen leeren Knoten, den Sie in eine Deployment Manager-Zelle einbinden müssen, damit dieser verwendet werden kann. Wenn Sie ein benutzerdefiniertes Profil einbinden, wird es zu einem verwalteten Knoten. Binden Sie einen Knoten nur ein, wenn der Deployment Manager, in den die Einbindung erfolgt, das gleiche oder ein höheres Release-Level als das benutzerdefinierte Profil aufweist, das von Ihnen erstellt wird.

Im Verzeichnis *installationsstammverzeichnis/profileTemplates/BusinessSpace* finden Sie Schablonen für die einzelnen Profile.

- b. Ermitteln Sie im Abschnitt „Befehlszeilendienstprogramm 'manageprofiles' (für Business Space-Profile)“ auf Seite 224, welche Parameter für die Profilerweiterung erforderlich sind. Ermitteln Sie die Werte, die Sie für das Profil

angeben möchten. Überprüfen Sie hierzu die Standardwerte, um festzustellen, ob diese bedarfsgerecht für Ihr Profil sind.

Sie verwenden den Parameter **augment**, um mit einer Erweiterungsschablone Änderungen an einem vorhandenen Profil durchzuführen. Der Parameter **augment** bewirkt, dass das Befehlszeilendienstprogramm **manageprofiles** das im Parameter **-profileName** angegebene Profil anhand der Schablone aktualisiert oder erweitert, die im Parameter **-templatePath** angegeben ist. Die Erweiterungsschablonen, die Sie verwenden können, sind von den IBM Produkten und den Versionen abhängig, die in Ihrer Umgebung installiert sind. Vergewissern Sie sich, dass Sie den vollständig qualifizierten Dateipfad für **-templatePath** angegeben haben, da ein relativer Dateipfad dazu führt, dass das angegebene Profil nicht vollständig erweitert werden kann.

- c. Führen Sie die Datei von der Befehlszeile aus. Im Folgenden finden Sie ein einfaches Beispiel:




```
manageProfiles -augment -profileName profilname
               -templatePath installationsstammverzeichnis/profileTemplates/BusinessSpace/managed.bspace
               -dmgrAdminUserName administratorname -dmgrAdminPassword administratorkennwort
               -dmgrPort deployment_manager-port -dmgrHost deployment_manager-hostname -cellName
               verwaltungszellenname -nodeName knotenname
```

Der Befehl zeigt bei seiner Ausführung den aktuellen Status an. Warten Sie, bis er beendet ist.

4. Melden Sie sich bei der Deployment Manager-Administrationskonsole an.
5. Optional: Wenn Sie noch über einen Cluster oder verwaltete Server verfügen, führen Sie eine der folgenden Aktionen für Ihre Umgebung aus:
  - Für einen Cluster:
    - a. Erstellen Sie einen Cluster von Anwendungsservern.
    - b. Fügen Sie ein oder mehr Cluster-Member zu dem Cluster hinzu (dies sind die angepassten Profile (Business Space), die zuvor erstellt wurden).
  - Für jeden verwalteten Server:
    - a. Erstellen Sie einen Anwendungsserver.
    - b. Wählen Sie den Knoten des verwalteten Servers als das angepasste Profil (Business Space) aus, das zuvor erstellt wurde.
6. Stoppen Sie das Deployment Manager-Profil.

Stoppen Sie den Deployment Manager mithilfe des Befehls `stopServer` im Verzeichnis `profilstammverzeichnis/bin`.

Verwenden Sie die folgende Syntax:

-   `stopServer.sh servername -username benutzername -password kennwort`
-  `stopServer.bat servername -username benutzername -password kennwort`

Wenn die Sicherheit für das Profil nicht aktiviert ist, sind die Parameter `-username` und `-password` nicht erforderlich.

Weitere Informationen zum Befehl `stopServer` finden Sie im Abschnitt zum Befehl `stopServer` im Information Center von WebSphere Application Server Version 8.0.

7. Navigieren Sie zum Verzeichnis `installationsstammverzeichnis/BusinessSpace/config.bspace/MetadataFiles` und kopieren Sie - abhängig von dem Datenbanktyp, den Sie für Business Space verwenden werden - die relevante Datei in ein Arbeitsverzeichnis. Ändern Sie die Erweiterung dieser Datei nicht: Sie muss `.properties` lauten.

- a. Bearbeiten Sie die Kopie dieser Datei und ändern Sie die Werte so, dass sie Ihrer Datenbank entsprechen. Achten Sie besonders auf die richtigen Einstellungen für die Eigenschaft `wasHome`.
- b. Wenn Sie die Datei bearbeitet und auf Ihre Datenbankinformationen abgestimmt haben, speichern Sie die Datei.

Wenn Sie die Profile erstellt und die Datenbankinformationen für Ihre Profile konfiguriert haben, können Sie Business Space in Ihrer Umgebung konfigurieren, indem Sie folgende Schritte ausführen:

1. Führen Sie für jeden Cluster oder für jeden verwalteten Server den Befehl **`installBusinessSpace`** aus, um die EAR-Dateien für Business Space in der Laufzeitumgebung zu installieren. Geben Sie entweder den Parameter **`clusterName`** oder die Parameter **`nodeName`** und **`serverName`** an, abhängig davon, wie Sie Ihre Network Deployment-Topologie einrichten. Vgl. „Business Space über die Befehlszeile konfigurieren“ auf Seite 251.
2. Führen Sie für jeden Cluster oder verwalteten Server den Befehl **`configureBusinessSpace`** aus. Geben Sie dazu entweder den Parameter **`clusterName`** oder die Parameter **`nodeName`** und **`serverName`** an, abhängig davon, wie Sie Ihre Network Deployment-Topologie einrichten. Geben Sie außerdem den Parameter **`bspacedbDesign`** an. Der Wert für diesen Parameter sollte der Pfad zu der Datei mit den Datenbankeigenschaften sein, die Sie zuvor bearbeitet haben. Optional können Sie bei der Erstellung von Datenbanktabellen und der Konfiguration der Business Space-Datenbank den Parameter **`createTables`** als wahr (`true`) angeben. Vgl. „Business Space über die Befehlszeile konfigurieren“ auf Seite 251.
3. Speichern Sie die `wsadmin`-Konfiguration.
4. Wurde der Parameter **`createTables`** in Schritt 2 nicht vorgegeben, erstellen und konfigurieren Sie die Business Space-Datenbank. Vgl. „Business Space-Datenbank konfigurieren“ auf Seite 255.
5. Starten Sie den Deployment Manager.
6. Starten Sie die Cluster oder verwalteten Server.

Wenn Sie ein Profil erweitern, für das die Sicherheit bereits mit einem Benutzerrepository einrichtet wurde (und zwar nicht die Standardoption für eingebundene Repositories), müssen Sie in der Datei `ConfigServices.properties` prüfen, ob der Parameter `MashupAdminForOOBSpace` angepasst werden muss. Vgl. „Benutzerrepository für Business Space auswählen“ auf Seite 282.

*Befehlszeilendienstprogramm 'manageprofiles' (für Business Space-Profil):*



Mit dem Befehlszeilendienstprogramm **`manageprofiles`** wird ein Profil erstellt. Dabei handelt es sich um eine Gruppe von Dateien, die die Laufzeitumgebung für einen Deployment Manager, einen verwalteten Knoten oder einen eigenständigen Server definieren. Sie können damit ein 'Business Space powered by WebSphere'-Profil erstellen. Wenn Business Space im Rahmen Ihres Produktprofils konfiguriert wird, sind diese Informationen optional.

Das Profil definiert die Laufzeitumgebung und umfasst alle Dateien, die von den Serverprozessen während der Laufzeit geändert werden können.

Nur über das Befehlszeilendienstprogramm **`manageprofiles`** und seine grafische Benutzerschnittstelle, das Profile Management Tool, können Profile und Laufzeitumgebungen erstellt werden. Mit dem Befehlszeilendienstprogramm **`manageprofiles`** können aber auch Profile erweitert und gelöscht werden.

Die Befehlsdatei befindet sich im Verzeichnis *installationsstammverzeichnis/bin*. Bei der Befehlsdatei handelt es sich um ein Script mit dem Namen *manageprofiles.sh* für Linux- und UNIX-Betriebssysteme bzw. *manageprofiles.bat* für Windows-Betriebssysteme.

Das Befehlszeilendienstprogramm **manageprofiles** erstellt ein Protokoll für jedes Profil, das mit diesem Befehlszeilendienstprogramm erstellt, gelöscht oder erweitert wird. Die Protokolle befinden sich je nach Betriebssystem im folgenden Verzeichnis:

-  *installationsstammverzeichnis/logs/manageprofiles*
-  *installationsstammverzeichnis\logs\manageprofiles*

Die folgenden Dateinamen werden verwendet:

- *profilname\_create.log*
- *profilname\_augment.log*
- *profilname\_delete.log*

Im Verzeichnis *installationsstammverzeichnis/profileTemplates/BusinessSpace* finden Sie Schablonen für die einzelnen Profile. Es enthält Unterverzeichnisse, die den verschiedenen Profiltypen entsprechen. Die Verzeichnisse entsprechen den Pfaden, die Sie dem Befehlszeilendienstprogramm **manageprofiles** mit der Option *-templatePath* übergeben. Es ist auch möglich, Profilschablonen anzugeben, die sich außerhalb des Installationsstammverzeichnisses befinden. Verwenden Sie für *BusinessSpace* die folgenden Schablonen:

- *default.bspace*: Für ein eigenständiges Serverprofil von *BusinessSpace*, das einen eigenständigen Server definiert.
- *dmgr.bspace*: Für ein Deployment Manager-Profil von *BusinessSpace*, das einen Deployment Manager definiert.
- *managed.bspace*: Für ein angepasstes (benutzerdefiniertes) Profil von *BusinessSpace*, das bei Einbindung in einen Deployment Manager einen verwalteten Knoten definiert.

## Syntax

Verwenden Sie das Befehlszeilendienstprogramm **manageprofiles**, um die folgenden Tasks auszuführen:

- Erstellung eines Profils (Parameter **-create**).
- Erweiterung eines Profils (Parameter **-augment**).

**Einschränkung:** Die Verwendung von Profilen, bei denen die Erweiterung aufgehoben wurde (Parameter **-unaugment**) wird nicht unterstützt.

- Löschen eines Profils (Parameter **-delete**).
- Löschen aller Profile (Parameter **-deleteAll**).
- Auflisten aller Profile (Parameter **-listProfiles**).
- Abrufen des Namens eines vorhandenen Profils anhand seines Namens (Parameter **-getName**).
- Abrufen des Namens eines vorhandenen Profils anhand seines Pfads (Parameter **-getPath**).
- Prüfen einer Profilregistry (Parameter **-validateRegistry**).
- Prüfen und Aktualisieren einer Profilregistry (Parameter **-validateAndUpdateRegistry**).

- Abrufen des Standardprofilnamens (Parameter **-getDefaultName**).
- Definieren des Standardprofilnamens (Parameter **-setDefaultName**).
- Sichern eines Profils (Parameter **-backupProfile**).
- Wiederherstellen eines Profils (Parameter **-restoreProfile**).
- Verwenden einer Antwortdatei mit den für die Ausführung des Befehlszeilendienstprogramms **manageprofiles** erforderlichen Informationen (Parameter **-response**).

Verwenden Sie den Parameter **-help**, um ausführliche Hilfe einschließlich der erforderlichen Parameter für die einzelnen Tasks, die mit dem Befehlszeilendienstprogramm **manageprofiles** ausgeführt werden, abzurufen. Das folgende Beispiel zeigt die Verwendung des Parameters **-help** mit dem Befehlszeilendienstprogramm **manageprofiles** und dem Parameter **-augment** auf Windows-Betriebssystemen: `manageprofiles.bat -augment -help`. Die Ausgabe gibt an, welche Parameter erforderlich und welche Parameter optional sind.

### Befehlsausgabe

Beim Befehlsabschluss wird eine Anweisung ähnlich einer der folgenden Nachrichten angezeigt. (Der genaue Wortlaut ist davon abhängig, ob Sie ein Profil erstellt, gelöscht oder erweitert haben.)

- **INSTCONFSUCCESS**: Die Profilerstellung war erfolgreich.
- **INSTCONFFAILED**: Profilerstellung fehlgeschlagen.
- **INSTCONFPARTIALSUCCESS**: Einige unkritische Konfigurationsaktionen nach der Installation waren nicht erfolgreich.

In einigen Fällen wird die Anweisung mehrfach angezeigt. Die Zeile **INSTCONFSUCCESS** wird beispielsweise dreimal in einer Befehlszeile angezeigt. Weitere Informationen finden Sie in "Protokolldateien zu Installation und Profilerstellung".

### Parameter

Bei der Erstellung eines BusinessSpace-Profiles sollten Sie nur die Parameter verwenden, die im Information Center für BusinessSpace dokumentiert sind. Bei allen Parametern muss die Groß-/Kleinschreibung beachtet werden.

#### **-adminUserName** *adminBenutzer\_ID*

Gibt die Benutzer-ID an, die für die administrative Sicherheit verwendet wird. Zur Erweiterung eines vorhandenen Profils, für das die administrative Sicherheit aktiviert ist, ist dieser Parameter erforderlich.

#### **-adminPassword** *adminKennwort*

Gibt das Kennwort der Benutzer-ID für die administrative Sicherheit an, die mit dem Parameter **-adminUserName** definiert wurde. Zur Erweiterung eines vorhandenen Profils, für das die administrative Sicherheit aktiviert ist, ist dieser Parameter erforderlich.

#### **-augment**

Verwenden Sie den Parameter **-augment**, um mit einer Erweiterungsschablone Änderungen an einem vorhandenen Profil durchzuführen. Der Parameter **-augment** bewirkt, dass das Befehlszeilendienstprogramm **manageprofiles** das im Parameter **-profileName** angegebene Profil anhand der Schablone aktualisiert oder erweitert, die im Parameter **-templatePath** angegeben ist. Die Erweiterungsschablonen, die Sie verwenden können, sind von den IBM Produkten und den Versionen abhängig, die in Ihrer Umgebung installiert sind.



**Wichtig:** Die Dateien, die sich im Verzeichnis *installationsverzeichnis/profileTemplates* befinden, dürfen nicht manuell geändert werden. Beispiel: Wenn Sie die Ports während der Profilerstellung ändern, verwenden Sie das Profile Management Tool oder das Argument **-startingPort** bzw. **-portsFile** des Befehlszeilendienstprogramms **manageprofiles**, anstatt die Datei im Profilschablonenverzeichnis zu ändern.

Geben Sie mit **-templatePath** den vollständig qualifizierten Dateipfad an. Beispiel: `manageprofiles(.bat)(.sh) -augment -profileName profilname -templatePath vollständig_qualifizierter_schablonenpfad`

**-backupProfile**

Führt eine Sicherung des Dateisystems für einen Profilordner und der Profilmetadata der Profilregistrydatei durch.

**-backupFile** *name\_sicherungsdatei*

Sichert die Profilregistrydatei in der angegebenen Datei. Sie müssen einen vollständig qualifizierten Dateipfad für die Datei *name\_sicherungsdatei* angeben.

**-bspacedbDesign** *datenbankentwurfsdatei*

Gibt den Pfad zur Business Space-Datenbankentwurfsdatei an. Musterentwurfsdateien finden Sie in folgendem Verzeichnis:

*installationsstammverzeichnis/BusinessSpace/config.bspace/MetadataFiles.*

**-bspaceSchemaName** *datenbankschemaname*

Der Schemaname für die Datenbank. Wenn kein Wert angegeben wurde, wird für die meisten Datenbanktypen der Wert `IBMBUSSP` verwendet.

**-cellName** *zellename*

Gibt den Zellennamen des Profils an. Verwenden Sie für jedes Profil einen eindeutigen Zellennamen. Geben Sie beim Erweitern eines Profils die Zelle des Originalprofils an. Der Standardwert für diesen Parameter basiert auf einer Kombination des Kurznamens für den Host, der Konstanten `Cell` und einer abschließenden Nummer.

Beispiel: `if (DMgr) shortHostNameCellZellenNummer`  
oder  
`shortHostNameNodeKnotenNummerCell`

Hierbei steht *ZellenNummer* für eine fortlaufende Zahl, die bei 01 beginnt, und *KnotenNummer* für die Knotennummer, die Sie zum Definieren des Knotennamens verwendet haben. Der Wert für diesen Parameter darf weder Leerzeichen noch die folgenden ungültigen Zeichen enthalten: `*`, `?`, `"`, `<`, `>`, `„`, `/`, `\` und `|`.

**-create**

Erstellt das Profil. Wenn Sie spezielle Informationen zur Erstellung eines Profils benötigen, dann geben Sie `manageprofiles -create -templatePath vollständig_qualifizierter_dateipfad_zur_schablone -help` ein. Die folgenden Schablonen sind verfügbar:

- `default.bspace`: Für ein eigenständiges Serverprofil von BusinessSpace, das einen eigenständigen Server definiert.
- `dmgr.bspace`: Für ein Deployment Manager-Profil von BusinessSpace, das einen Deployment Manager definiert.
- `managed.bspace`: Für ein angepasstes (benutzerdefiniertes) Profil von BusinessSpace, das bei Einbindung in einen Deployment Manager einen verwalteten Knoten definiert.
- 

**-dbBspacePassword** *bpace-db-kennwort*

Dieser Parameter ist erforderlich, wenn Sie während der Profilerstellung einen

benutzerdefinierten Benutzernamen mit zugehörigem Kennwort eingeben und den Wert ORACLE für den Parameter **-dbType** angeben. Der Standardwert ist dbPassword.

**-dbBspaceUserId** *bospace-db-benutzer-id*

Dieser Parameter ist erforderlich, wenn Sie während der Profilerstellung einen benutzerdefinierten Benutzernamen mit zugehörigem Kennwort eingeben. Der Standardwert lautet IBMBUSSP.

**-dbConnectionLocation** *db2-position*

Die Position, an der sich die DB2 for z/OS-Datenbank befindet.

**-dbCreateNew**

Gibt an, ob eine neue Datenbank erstellt oder eine bereits vorhandene Datenbank wiederverwendet werden soll. Gültige Werte sind true und false. Der Standardwert ist true (wahr).

**-dbDelayConfig**

Gibt an, ob die Tabellenerstellung auf einen Zeitpunkt nach der Profilerstellung verlegt werden soll. Gültige Werte sind true und false. Der Standardwert ist false (falsch). Setzen Sie diesen Parameter auf den Wert true, um die Ausführung von Datenbankskripts zu verzögern, wenn eine ferne Datenbank verwendet wird.

**-dbDriverType** *db-treibertyp*

Der Typ des Datenbanktreibers, der nur für Oracle gültig ist. Geben Sie bei einer Oracle-Datenbank den Wert ORACLE an. Bei anderen Datenbanken als Oracle wird dieser Wert abhängig vom Serverbetriebssystem automatisch gesetzt. Serverinstallationen unter z/OS verwenden den Typ 2. Serverinstallationen unter allen anderen Betriebssystemen verwenden den Typ 4.

**-dbDriverVersion** *db-treiberversion*

Die Version des Datenbanktreibers, die nur für Microsoft SQL Server gültig ist. Geben Sie bei einer SQL Server-Datenbank entweder 1.2 für den Microsoft-SQL-JDBC-Treiber 1.2 oder 2.0 für den Microsoft-SQL-JDBC-Treiber 2.0 an. Bei Nichtangabe dieses Werts wird automatisch der Standardwert 2.0 verwendet.

**-dbHostName** *db-hostname*

Der Hostname oder die IP-Adresse des Datenbankservers. Der Standardwert lautet localhost.

**-dbJDBCClasspath** *jdbc-treiberposition*

Die Position der Dateien des JDBC-Treibers. Sie müssen den Treiber ojdbc6.jar installieren, um auf die Oracle-Datenbank zuzugreifen. Oracle 10g enthält den Treiber ojdbc6.jar nicht. Sie können ihn von der Website für Oracle herunterladen.

**-dbName** *db-name*

Der Name der Datenbank. Standardmäßig ist hierfür bei Oracle-Datenbanken der Wert orc1 und bei allen übrigen unterstützten Datenbanken der Wert BSPACE festgelegt.

**-dbPassword** *db-kennwort*

Das Kennwort, das für die gesamte Datenbankauthentifizierung erforderlich ist.

**-dbServerPort** *db-portnummer*

Dieser Parameter gibt die Portnummer des Datenbankservers an. Abhängig von der verwendeten Datenbank können Sie anstelle der Standardportnummer auch eine andere Portnummer angeben.

**-dbStorageGroup** *db-speichergruppe*

Der Name der Speichergruppe für DB2 for z/OS-Datenbanken.

**-dbSysPassword** *sys-kennwort*

Verwenden Sie dieser Parameter, wenn für den Parameter **dbDelayConfig** der Wert 'false' festgelegt ist und Sie für **dbType** den Wert ORACLE angegeben haben. Dieser Parameter ist optional. Bei Nichtangabe wird das Oracle-Schema nicht erstellt.

**-dbSysUserId** *sys-benutzer-ID*

Diese ID muss über SYSDBA-Berechtigungen verfügen. Verwenden Sie nicht den Oracle-internen Benutzer sys. Verwenden Sie dieser Parameter, wenn für den Parameter **dbDelayConfig** der Wert 'false' festgelegt ist und Sie für **dbType** den Wert ORACLE angegeben haben. Dieser Parameter ist optional. Bei Nichtangabe wird das Oracle-Schema nicht erstellt.

**-dbType** *db-typ*

Der Datenbanktyp. Definieren Sie einen der folgenden Werte für den Typ des Datenbankprodukts, das von Ihnen zusammen mit Business Space eingesetzt wird.

- DB2 Universal = DB2\_Universal
- DB2 DataServer = DB2\_DataServer
- DB2 Universal for z/OS = DB2UDBOS390
- Oracle = Oracle
- Microsoft SQL Server = MSSQLSERVER\_MICROSOFT

**-dbUserId** *db-benutzer-id*

Benutzer-ID für alle Datenbanktypen. Gibt die Benutzer-ID an, die über Berechtigungen zum Erstellen und Löschen der Datenbanken verfügt. Die WebSphere-Datenquelle verwendet diese ID zur Authentifizierung der Datenbankverbindung. Bei DB2-Datenbanken gibt sie die Benutzer-ID des Datenbankbenutzers an, der als Eigner der Datenbanktabellen fungieren wird. Für DB2 for z/OS-Datenbanken wird die Benutzer-ID angegeben, die über Berechtigungen zum Erstellen und Löschen von Datenbanken verfügt. Dieser Parameter ist erforderlich. Wichtig: Der Wert für den Parameter **-dbUserId** muss eine gültige Datenbankberechtigungs-ID sein. Weitere Informationen zu Berechtigungs-IDs finden Sie im Abschnitt zu Berechtigungs-IDs und Berechtigungs-namen auf der Seite zu Einschränkungen bei DB2-Eigenschaften.

**-dbWinAuth** *true|false*

Gibt an, ob Sie Windows-Authentifizierung mit Microsoft SQL Server verwenden. Wenn Sie die Windows-Authentifizierung in Ihrer SQL-Serverumgebung verwenden möchten, müssen Sie den Parameter auf true setzen. Der Standardwert ist false.

**-debug**

Aktiviert die Debugfunktion des Apache Ant-Dienstprogramms, das das Befehlszeilendienstprogramm **manageprofiles** verwendet.

**-defaultPorts**

Ordnet dem Profil die Standard- oder Basisportwerte zu.

Verwenden Sie diesen Parameter nicht, wenn Sie den Parameter **-startingPort** oder **-portsFile** benutzen wollen.

Während der Profilerstellung verwendet das Befehlszeilendienstprogramm **manageprofiles** eine automatisch generierte Gruppe empfohlener Ports, wenn Sie den Parameter **-startingPort**, **-defaultPorts** oder **-portsFile** nicht an-

geben. Die empfohlenen Portwerte können abhängig von der Verfügbarkeit der Standardports von den Standardportwerten abweichen.

**Anmerkung:** Verwenden Sie diesen Parameter nicht, wenn Sie mit der Schablone für verwaltete Profile arbeiten.

#### **-delete**

Löscht das Profil.

Durch das Löschen eines Profils wird das Profilverzeichnis nicht gelöscht. Wenn Sie zum Beispiel ein Profil im Verzeichnis `/usr/WebSphere/AppServer/profiles/AppSrvr01` erstellen, so bleibt das Verzeichnis auch nach dem Löschen des Profils bestehen.

Sie können das Verzeichnis dann löschen oder auf dem System belassen. Das Verzeichnis `profilstammverzeichnis/logs` enthält Informationen zur Deinstallation des Profils. Sie können beispielsweise die Datei `_nodeuninst.log` beibehalten, um die Ursache eines Problems zu ermitteln, das während der Deinstallation aufgetreten ist.

Wenn Sie ein Profil löschen, für das in der Profilregistry Erweiterungsschablonen registriert wurden, dann werden die Aktionen zur Aufhebung der Erweiterung automatisch ausgeführt.

#### **-deleteAll**

Löscht alle registrierten Profile.

Durch das Löschen eines Profils wird das Profilverzeichnis nicht gelöscht. Wenn Sie zum Beispiel ein Profil im Verzeichnis `/usr/WebSphere/AppServer/profiles/AppSrvr01` erstellen, so bleibt das Verzeichnis auch nach dem Löschen des Profils bestehen.

Sie können das Verzeichnis dann löschen oder auf dem System belassen. Das Verzeichnis `profilstammverzeichnis/logs` enthält Informationen zur Deinstallation des Profils. Sie können beispielsweise die Datei `_nodeuninst.log` beibehalten, um die Ursache eines Problems zu ermitteln, das während der Deinstallation aufgetreten ist.

Wenn Sie ein Profil löschen, für das in der Profilregistry Erweiterungsschablonen registriert wurden, dann werden die Aktionen zur Aufhebung der Erweiterung automatisch ausgeführt.

#### **-dmgrAdminUserName** *benutzername*

Wenn die Verwaltungssicherheit auf dem Deployment Manager aktiviert ist, geben Sie einen gültigen Benutzernamen an.

#### **-dmgrAdminPassword** *kennwort*

Wenn die Verwaltungssicherheit auf dem Deployment Manager aktiviert ist, geben Sie ein Kennwort für den Benutzernamen an.

#### **-dmgrHost** *deployment\_manager-hostname*

Identifiziert die Workstation, auf der der Deployment Manager aktiv ist. Geben Sie diesen Parameter in Verbindung mit dem Parameter **dmgrPort** an, um ein benutzerdefiniertes Profil bei seiner Erstellung oder Erweiterung einzubinden. Dieser Parameter steht zusammen mit der Profilschablone `'managed.bspace'` zur Verfügung.

Für den Hostnamen kann der lange oder der kurze DNS-Name oder die IP-Adresse der Workstation mit dem Deployment Manager verwendet werden.

Durch Angabe dieses optionalen Parameters versucht das Befehlszeilendienstprogramm **manageprofiles**, den benutzerdefinierten Knoten im Rahmen der Er-

stellung des benutzerdefinierten Profils in die Deployment Manager-Zelle einzubinden. Bei der Erstellung eines Deployment Manager-Profiles oder eines eigenständigen Serverprofils wird dieser Parameter ignoriert.

Wenn Sie einen benutzerdefinierten Knoten einbinden, während der Deployment Manager nicht aktiv ist, dann wird mit der Installationsanzeige `INSTCONFFAILED` in den Protokollen das vollständige Fehlschlagen der Installation dokumentiert. Das entstandene benutzerdefinierte Profil ist nicht verwendbar. Bevor Sie ein weiteres benutzerdefiniertes Profil mit dem gleichen Profilnamen erstellen, müssen Sie das Verzeichnis des benutzerdefinierten Profils aus dem Profilrepository (dem Installationsstammverzeichnis des Profils) verschieben.

Wenn Sie den Standardtyp des JMX-Connectors geändert haben, können Sie das Befehlszeilendienstprogramm `manageprofiles` nicht zum Einbinden verwenden. Verwenden Sie stattdessen den Befehl `addNode`.

Der Standardwert für diesen Parameter ist `localhost`. Als Wert für diesen Parameter muss ein korrekt formatierter Hostname angegeben werden, der weder Leerzeichen noch die folgenden ungültigen Zeichen enthalten darf: `*`, `?`, `"`, `<`, `>`, `,`, `/`, `\` und `|`. Wenn der Parameter `dmgrPort` verwendet wird, muss außerdem eine Verbindung zum Deployment Manager verfügbar sein.

**-dmgrPort** *deployment\_manager-portnummer*

Identifiziert den SOAP-Port des Deployment Managers. Geben Sie diesen Parameter in Verbindung mit dem Parameter `dmgrHost` an, um ein benutzerdefiniertes Profil bei seiner Erstellung oder Erweiterung einzubinden. Der Deployment Manager muss aktiv und erreichbar sein.

Wenn den standardmäßigen JMX-Connector-Typ geändert haben, können Sie das Befehlszeilendienstprogramm `manageprofiles` nicht zum Einbinden verwenden. Verwenden Sie stattdessen den Befehl `addNode`.

Der Standardwert für diesen Parameter ist `8879`. Für den Port müssen Sie eine positive ganze Zahl angeben. Außerdem muss bei Verwendung des Parameters `dmgrHost` eine Verbindung zum Deployment Manager verfügbar sein.

**-enableAdminSecurity** *true | false*

Aktiviert die administrative Sicherheit. Die gültigen Werte lauten `true` und `false`. Der Standardwert lautet `false`. Wenn Sie Profile für eine Implementierungsumgebung erstellen, müssen Sie diesen Parameter auf `true` setzen. Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

Wenn der Parameter `enableAdminSecurity` auf den Wert `true` eingestellt ist, müssen Sie außerdem die Parameter `-adminUserName` und `-adminPassword` sowie die Werte für diese Parameter angeben. Wenn während der Anwendungsserverinstallation auch Beispielemente installiert wurden, müssen Sie auch den Parameter `-samplesPassword` angeben, wenn Sie ein Profil erstellen wollen, für das die administrative Sicherheit aktiviert ist. Wenn der Parameter `-samplesPassword` nicht angegeben, die administrative Sicherheit jedoch aktiviert wird, dann kann das Profil zwar erfolgreich erstellt werden, beim Ausführen der Beispiele werden jedoch Ausnahmebedingungen und Fehler im Systemausgabeprotokoll des Servers aufgezeichnet.

**> Linux**

**-enableService** *true | false*

Aktiviert die Erstellung eines Linux-Service. Die gültigen Werte lauten `true` und `false`. Der Standardwert für diesen Parameter lautet `false`. Verwenden Sie

diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

Wenn das Befehlszeilendienstprogramm **manageprofiles** mit der Option **-enableService** ausgeführt wird und für diese der Wert **true** eingestellt ist, dann wird der Linux-Service mit dem Profil erstellt, wenn der Befehl vom Rootbenutzer ausgeführt wird. Wenn ein Benutzer ohne Rootberechtigung das Befehlszeilendienstprogramm **manageprofiles** ausführt, wird das Profil zwar erstellt, der Linux-Service jedoch nicht. Der Linux-Service wird nicht erstellt, weil der Benutzer ohne Rootberechtigung nicht über die erforderlichen Berechtigungen zum Definieren des Service verfügt. Am Ende der Profilerstellung wird das Ergebnis **INSTCONPARTIALSUCCESS** angezeigt. Das Profilerstellungsprotokoll *installationsstamverzeichnis/logs/manageprofiles/profilename\_create.log* enthält eine Nachricht, in der angegeben ist, dass der aktuelle Benutzer nicht über die Berechtigungen zum Definieren des Linux-Service verfügt.

**-federateLater true | false**

Gibt an, ob das verwaltete Profil während der Profilerstellung eingebunden wird oder ob Sie das Profil zu einem späteren Zeitpunkt mit dem Befehl **addNode** einbinden. Wenn Sie ein Business Space-Profil erstellen, dann geben Sie keinen Wert an. Verwenden Sie stattdessen den Standardwert **true**.

**-getDefaultName**

Gibt den Namen des Standardprofils zurück.

**-getName**

Ruft den Namen eines Profils ab, das mit einem bestimmten Parameter **-profilePath** registriert wurde.

**-getPath**

Ruft die Position des Dateisystems für ein Profil eines bestimmten Namens ab. Dafür ist der Parameter **profileName** erforderlich.

**-help**

Zeigt die Befehlssyntax an.

**-hostName hostname**

Gibt den Namen des Hosts an, auf dem das Profil erstellt wird. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern. Dieser Wert sollte mit dem Hostnamen übereinstimmen, den Sie während der Erstinstallation des Produkts angegeben haben. Der Standardwert für diesen Parameter ist die Langform des Domännennamenssystems. Dieser Parameter ist nur für die Profilerstellung erforderlich. Als Wert für diesen Parameter muss ein gültiger IPv6-Hostname angegeben werden. Dieser darf weder Leerzeichen noch die folgenden ungültigen Zeichen enthalten: **\***, **?**, **"**, **<**, **>**, **,**, **/**, **\** und **|**.

**-importPersonalCertKS keystore-pfad**

Gibt den Pfad zu der Keystore-Datei an, die Sie beim Erstellen eines Profils zum Importieren eines persönlichen Zertifikats verwenden. Das persönliche Zertifikat ist das standardmäßige persönliche Zertifikat des Servers.

Wenn Sie ein persönliches Zertifikat als persönliches Standardzertifikat importieren, importieren Sie das Stammzertifikat, mit dem das persönliche Zertifikat signiert wurde. Ansonsten fügt das Dienstprogramm **manageprofiles** den öffentlichen Schlüssel des persönlichen Zertifikats zur Datei **trust.p12** hinzu und erstellt ein Stammsignaturzertifikat.

Die Parameter **-importPersonalCertKS** und **-personalCertDN** schließen sich gegenseitig aus. Wenn Sie nicht ausdrücklich ein persönliches Zertifikat erstellen oder importieren, so wird standardmäßig eines erstellt.



Wenn Sie auch nur einen der Parameter angeben, die mit `-importPersonal` beginnen, so müssen Sie sie alle angeben.

**`-importPersonalCertKSType`** *keystore-typ*

Gibt den Typ von Keystore-Datei an, die Sie mit dem Parameter `-importPersonalCertKS` angeben. Mögliche Werte sind JCEKS, CMSKS, PKCS12, PKCS11 und JKS. Diese Liste kann sich jedoch abhängig von dem in der Datei `java.security` angegebenen Provider ändern.

Wenn Sie auch nur einen der Parameter angeben, die mit `-importPersonal` beginnen, so müssen Sie sie alle angeben.

**`-importPersonalCertKSPassword`** *keystore-kennwort*

Gibt das Kennwort für die Keystore-Datei an, die Sie mit dem Parameter `-importPersonalCertKS` angeben.

Wenn Sie auch nur einen der Parameter angeben, die mit `-importPersonal` beginnen, so müssen Sie sie alle angeben.

**`-importPersonalCertKSALias`** *keystore-alias*

Gibt den Aliasnamen des Zertifikats in der Keystore-Datei an, die Sie mit dem Parameter `-importPersonalCertKS` angeben. Das Zertifikat wird zu der standardmäßigen Keystore-Datei des Servers hinzugefügt und als standardmäßiges persönliches Zertifikat für den Server verwendet.

Wenn Sie auch nur einen der Parameter angeben, die mit `-importPersonal` beginnen, so müssen Sie sie alle angeben.

**`-importSigningCertKS`** *keystore-pfad*

Gibt den Pfad zu der Keystore-Datei an, die Sie beim Erstellen eines Profils zum Importieren eines Stammzertifikats verwenden. Das Stammzertifikat ist das Zertifikat, das Sie als standardmäßiges Stammzertifikat für den Server verwenden. Die Parameter `-importSigningCertKS` und `-signingCertDN` schließen sich gegenseitig aus. Wenn Sie nicht ausdrücklich ein Stammsignaturzertifikat erstellen oder importieren, so wird standardmäßig eines erstellt.

Wenn Sie auch nur einen der Parameter angeben, die mit `-importSigning` beginnen, müssen Sie sie alle angeben.

**`-importSigningCertKSType`** *keystore-pfad*

Gibt den Typ von Keystore-Datei an, die Sie mit dem Parameter `-importSigningCertKS` angeben. Gültige Werte sind JCEKS, CMSKS, PKCS12, PKCS11 und JKS. Diese Liste kann sich jedoch abhängig von dem in der Datei `java.security` angegebenen Provider ändern.

Wenn Sie auch nur einen der Parameter angeben, die mit `-importSigning` beginnen, so müssen Sie sie alle angeben.

**`-importSigningCertKSPassword`** *keystore-kennwort*

Gibt das Kennwort für die Keystore-Datei an, die Sie mit dem Parameter `-importSigningCertKS` angeben.

Wenn Sie auch nur einen der Parameter angeben, die mit `-importSigning` beginnen, so müssen Sie sie alle angeben.

**`-importSigningCertKSALias`** *keystore-alias*

Gibt den Aliasnamen des Zertifikats in der Keystore-Datei an, die Sie mit dem Parameter `-importSigningCertKS` angeben. Das Zertifikat wird zum standardmäßigen Stamm-Keystore des Servers hinzugefügt und als standardmäßiges persönliches Zertifikat für den Server verwendet.

Wenn Sie auch nur einen der Parameter angeben, die mit `-importSigning` beginnen, so müssen Sie sie alle angeben.

**-isDefault**

Gibt an, dass das im zugehörigen Parameter **-profileName** angegebene Profil nach seiner Registrierung als Standardprofil verwendet werden soll. Bei der Eingabe von Befehlen, in denen das Standardprofil aufgeführt wird, ist es nicht erforderlich, das Attribut **-profileName** des Befehls zu verwenden.

**-keyStorePassword** *keyStore-kennwort*

Gibt das Kennwort an, das für alle Keystore-Dateien verwendet werden soll, die während der Profilerstellung erstellt wurden. Keystore-Dateien werden für das standardmäßige persönliche Zertifikat und für das Stammsignaturzertifikat erstellt.

**-listAugments**




Listet die registrierten Erweiterungen für ein Profil auf, das sich in der Profilvergistry befindet. Der Parameter **-profileName** muss zusammen mit dem Parameter **-listAugments** angegeben werden.

**-listProfiles**

Listet alle definierten Profile auf.

**-nodeName** *knotenname*

Gibt den Knotennamen für den Knoten an, der mit dem neuen Profil erstellt wird. Verwenden Sie einen Wert, der innerhalb der Zelle oder auf der Workstation eindeutig ist. Jedes Profil, das an der gemeinsamen Nutzung derselben Gruppe von Produktbinärdateien beteiligt ist, muss einen eindeutigen Knotennamen aufweisen. Geben Sie beim Erweitern eines Profils den Knoten des Originalprofils an.

   Der Standardwert für diesen Parameter basiert auf dem Kurznamen für den Host, dem Profiltyp und einer abschließenden Nummer. Beispiel:

Beispiel: `if (DMgr)`  
`kurzname_für_hostCellManagerKnotenNummer`  
 oder  
`kurzname_für_hostNodeKnotenNummer`

Hierbei steht *KnotenNummer* für eine fortlaufende Zahl, die bei 01 beginnt.

Der Wert für diesen Parameter darf weder Leerzeichen noch die folgenden ungültigen Zeichen enthalten: \*, ?, ", <, >, ,, /, \ und |, .

**-omitAction** *feature1 feature2... featureN*

Ein optionaler Parameter, mit dem bestimmte Profilfeatures ausgeschlossen werden können.

Jede Profilschablone verfügt über bestimmte vordefinierte optionale Features. Die Option **samplesInstallAndConfig** steht nur zur Verfügung, wenn das Produkt mit ausgewählten Musteranwendungen installiert wird. Die folgenden optionalen Features können beim Parameter **-omitAction** für die folgenden Profilschablonen verwendet werden:

- **default** - Anwendungsserver
  - deployAdminConsole
  - samplesInstallAndConfig
  - defaultAppDeployAndConfig
- **dmgr** - Deployment Manager
  - deployAdminConsole

**-personalCertDN** *definiertes\_name*

Gibt den definierten Namen des persönlichen Zertifikats an, das Sie beim Er-

stellen des Profils erstellen. Geben Sie den definierten Namen in Anführungszeichen an. Dieses standardmäßige persönliche Zertifikat befindet sich in der Keystore-Datei des Servers. Die Parameter **-importPersonalCertKSType** und **-personalCertDN** schließen sich gegenseitig aus. Weitere Informationen finden Sie bei den Parametern **-personalCertValidityPeriod** und **-keyStorePassword**.

**-personalCertValidityPeriod** *gültigkeitszeitraum*

Dieser Parameter ist optional und gibt den Gültigkeitszeitraum des standardmäßigen persönlichen Zertifikats in Jahren an. Wenn Sie diesen Parameter nicht zusammen mit dem Parameter **-personalCertDN** angeben, hat das standardmäßige persönliche Zertifikat eine Gültigkeit von einem Jahr.

**-portsFile** *dateipfad*

Ein optionaler Parameter, der den Pfad zu einer Datei angibt, in der Porteinstellungen für das neue Profil definiert werden. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

Verwenden Sie diesen Parameter nicht, wenn Sie den Parameter **-startingPort** oder **-defaultPorts** benutzen wollen.

Während der Profilerstellung verwendet das Befehlszeilendienstprogramm **manageprofiles** eine automatisch generierte Gruppe empfohlener Ports, wenn Sie den Parameter **-startingPort**, **-defaultPorts** oder **-portsFile** nicht angeben. Die empfohlenen Portwerte können abhängig von der Verfügbarkeit der Standardports von den Standardportwerten abweichen.

**-profileName** *profilname*

Gibt den Namen des Profils an. Verwenden Sie zum Erstellen eines Profils einen eindeutigen Wert.

Jedes Profil, das an der gemeinsamen Nutzung derselben Gruppe von Produktbinärdateien beteiligt ist, muss einen eindeutigen Namen aufweisen. Der Standardprofilname basiert auf dem Profiltyp und weist eine abschließende Nummer auf. Beispiel:

*profilTyp ProfilNummer*

Hierbei steht *profilTyp* für einen Wert wie beispielsweise *AppSrv*, *Dmgr* oder *Custom* und *ProfilNummer* für eine fortlaufende Zahl, mit der ein eindeutiger Profilname erstellt wird.

Der Wert für diesen Parameter darf weder Leerzeichen noch die folgenden ungültigen Zeichen enthalten: \*, ?, ", <, >, ,, /, \ und |. Der Profilname, den Sie auswählen, darf noch nicht belegt sein.


**-profilePath** *profilstammverzeichnis*

Gibt den vollständig qualifizierten Pfad des Profils an, auf den im Information Center als *profilstammverzeichnis* verwiesen wird.

Beispiel:

**-profilePath** *profilstammverzeichnis*

Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

 **Unter Windows-Betriebssystemen:** Wenn der vollständig qualifizierte Pfad Leerzeichen enthält, dann schließen Sie die Angabe in Anführungszeichen ein.

Der Standardwert basiert auf dem Verzeichnis *installationsstammverzeichnis*, dem Unterverzeichnis für Profile und dem Namen der Datei.

Beispiel: Der Standardwert für die Profilerstellung lautet wie folgt:

*WS\_WSPROFILE\_DEFAULT\_PROFILE\_HOME/profilName*

Hierbei ist *WS\_WSPROFILE\_DEFAULT\_PROFILE\_HOME* in der Datei *wasprofile.properties* im Verzeichnis *installationsstammverzeichnis/properties* definiert.

Als Wert für diesen Parameter muss ein gültiger Pfad für das Zielsystem angegeben werden, der momentan noch nicht belegt ist.

Sie müssen außerdem über Schreibberechtigung für das Verzeichnis verfügen.

#### **-response** *antwortdatei*

Greift über die Befehlszeile mit dem Befehlszeilendienstprogramm **manageprofiles** auf alle API-Funktionen zu.

Die Befehlszeilenschnittstelle kann über eine Antwortdatei gesteuert werden, die die Eingabeargumente für einen bestimmten Befehl in der Merkmaldatei im Schlüssel/Wert-Format enthält. Im Folgenden ist eine Musterantwortdatei aufgeführt, die für eine Erstellungsoperation eingesetzt werden kann:

```
create
profileName=testResponseFileCreate
profilePath=profilstammverzeichnis
templatePath=installationsstammverzeichnis/profileTemplates/default
nodeName=myNodeName
cellName=myCellName
hostName=myHostName
omitAction=myOptionalAction1, myOptionalAction2
```

**Windows** **Unter Windows-Betriebssystemen:** In der Pfadanweisung unter dem Windows-Betriebssystem können entweder Schrägstriche (/) oder Backslashes (\) verwendet werden. Wenn in der Pfadanweisung Backslashes verwendet werden, dann müssen in der Antwortdatei doppelte Backslashes angegeben werden, da die Pfadangabe sonst von der Antwortdatei nicht korrekt interpretiert werden kann. Im Folgenden ist ein Beispiel einer Antwortdatei für eine Erstellungsoperation aufgeführt, in der doppelte Backslashes verwendet werden:

```
create
templatePath=C:\\WebSphere\\AppServer\\profileTemplates\\BusinessSpace\\default.bspace
```

Beim Hinzufügen von Merkmalen, die definierte Namen von Zertifikaten angeben, müssen vor Kommas doppelte Backslashes (\\) stehen. Beachten Sie, dass als Trennzeichen zwischen dem Schlüssel (*personalCertDN*) und dem Wert kein Gleichheitszeichen sondern ein Leerzeichen verwendet werden muss. Dies ist deshalb erforderlich, da das Gleichheitszeichen in dem Merkmalwert vorkommt. Im Folgenden ist ein Beispiel einer Antwortdateianweisung für einen Zertifikatseintrag aufgeführt, in der doppelte Backslashes verwendet werden:

```
personalCertDN cn=machine_name.dnx_suffix.com\\,ou=systemname
Node04Cell\\,ou=systemnameNode04\\,o=IBM\\,c=US
```

Um festzustellen, welche Eingabeargumente für die verschiedenen Typen von Profilschablonen und Aktionen erforderlich sind, verwenden Sie das Befehlszeilendienstprogramm **manageprofiles** mit dem Parameter **-help**.

#### **-restoreProfile**

Schreibt die Sicherungskopie eines Profils zurück. Dieser Parameter muss zusammen mit dem Parameter **-backupFile** verwendet werden.

#### **-samplesPassword** *beispielKennwort*

Erstellt ein Kennwort, das für die Beispiele verwendet wird. Das Kennwort dient zur Einschränkung des Zugriffs auf die Webanwendungsbeispiele, die während der Installation des Anwendungsservers installiert wurden.

**-serverType DEPLOYMENT\_MANAGER**

Gibt den Typ von Verwaltungsprofil an. Geben Sie DEPLOYMENT\_MANAGER für ein Verwaltungsprofil an. Dieser Parameter ist erforderlich, wenn ein Verwaltungsprofil erstellt wird.

**> Linux**

**-serviceUserName service\_benutzer-id**

Gibt die Benutzer-ID an, die während der Erstellung des Linux-Service verwendet wird, sodass der Linux-Service unter dieser Benutzer-ID ausgeführt wird. Der Linux-Service wird immer ausgeführt, wenn die Benutzer-ID angemeldet ist.

**-setDefaultName**

Legt als Standardprofil eines der vorhandenen Profile fest. Dieser Parameter muss zusammen mit dem Parameter `-profileName` verwendet werden. Beispiel:  
`manageprofiles(.bat)(.sh) -setDefaultName -profileName profilname`

**-signingCertDN definierter\_name**

Gibt den definierten Namen des Stammsignaturzertifikats an, das Sie beim Erstellen des Profils erstellen. Geben Sie den definierten Namen in Anführungszeichen an. Dieses standardmäßige persönliche Zertifikat befindet sich in der Keystore-Datei des Servers. Die Parameter `-importSigningCertKS` und `-signingCertDN` schließen sich gegenseitig aus. Wenn Sie nicht ausdrücklich ein Stammsignaturzertifikat erstellen oder importieren, so wird standardmäßig eines erstellt. Weitere Informationen finden Sie bei den Parametern `-signingCertValidityPeriod` und `-keyStorePassword`.

**-signingCertValidityPeriod gültigkeitszeitraum**

Dieser Parameter ist optional und gibt den Gültigkeitszeitraum des Stammsignaturzertifikats in Jahren an. Wenn Sie diesen Parameter nicht zusammen mit dem Parameter `-signingCertDN` angeben, hat das Stammsignaturzertifikat eine Gültigkeit von 20 Jahren.

**-startingPort anfangsport**

Gibt die Nummer des Anfangsports für die Generierung und die Zuordnung aller anderen Ports für das Profil an.

Definieren Sie diesen Parameter nicht, wenn Sie ein bereits vorhandenes Profil erweitern. Portwerte werden fortlaufend beginnend bei dem für **-startingPort** angegebenen Wert zugeordnet. Dabei werden die Ports übergangen, die bereits belegt sind. Das System erkennt und löst die gegenwärtig belegten Ports auf und bestimmt die Portzuordnungen, um Portkonflikte zu vermeiden.

Verwenden Sie diesen Parameter nicht zusammen mit dem Parameter **-defaultPorts** oder **-portsFile**.

Während der Profilerstellung verwendet das Befehlszeilendienstprogramm **manageprofiles** eine automatisch generierte Gruppe empfohlener Ports, wenn Sie den Parameter **-startingPort**, **-defaultPorts** oder **-portsFile** nicht angeben. Die empfohlenen Portwerte können abhängig von der Verfügbarkeit der Standardports von den Standardportwerten abweichen.

**Anmerkung:** Verwenden Sie diesen Parameter nicht, wenn Sie mit der Schablone für verwaltete Profile arbeiten.

**-templatePath schablonenpfad**

Gibt den Verzeichnispfad zu den Schablonendateien im Installationsstammverzeichnis an. Im Verzeichnis `profileTemplates` befinden sich verschiedene Verzeichnisse, die den unterschiedlichen Profiltypen zugeordnet sind und ab-

hängig vom installierten Produkt variieren können. Die Profilverzeichnisse entsprechen den Pfaden, die Sie bei der Verwendung der Option **-templatePath** angeben. Sie können Profilschablonen angeben, die sich außerhalb des Installationsstammverzeichnisses befinden, wenn Sie über solche Schablonen verfügen.

Verwenden Sie absolute Pfade. Dieser Parameter muss als Verzeichnis vorhanden sein und auf ein gültiges Schablonenverzeichnis verweisen. Verwenden Sie für Business Space die folgenden Schablonen:

- **default.bspace**: Für ein eigenständiges Serverprofil (Business Space), das einen eigenständigen Server definiert.
- **dmgr.bspace**: Für ein Deployment Manager-Profil (Business Space), das einen Deployment Manager definiert.
- **managed.bspace**: Für ein angepasstes (benutzerdefiniertes) Profil (Business Space), das bei Einbindung in einen Deployment Manager einen verwalteten Knoten definiert.

#### **-validateAndUpdateRegistry**

Überprüft alle Profile, die in der Profilregistry aufgelistet werden, um festzustellen, ob die Profile im Dateisystem vorhanden sind. Entfernt alle fehlenden Profile aus der Registry. Gibt eine Liste der fehlenden Profile zurück, die aus der Registry gelöscht wurden.

#### **-validateRegistry**

Überprüft alle Profile, die in der Profilregistry aufgelistet werden, um festzustellen, ob die Profile im Dateisystem vorhanden sind. Gibt eine Liste der fehlenden Profile zurück.

#### **-validatePorts**

Gibt die Ports an, die überprüft werden sollen, um sicherzustellen, dass diese nicht reserviert oder belegt sind. Verwenden Sie diesen Parameter, um Ports zu ermitteln, die nicht belegt sind. Wenn ein Port als belegt identifiziert wird, dann wird die Profilerstellung gestoppt und eine Fehlermeldung ausgegeben. Sie können diesen Parameter jederzeit in der Befehlszeile des Erstellungsbefehls verwenden. Es wird empfohlen, diesen Parameter zusammen mit dem Parameter **portsFile** zu verwenden.

#### **-webFormConfig true | false**

Gibt an, ob Business Space für die Verwendung von IBM Forms Server zur Arbeit mit den Widgets für die Benutzertaskverwaltung konfiguriert ist. Der Standardwert für diesen Parameter lautet **false**. Geben Sie **true** an, um Business Space für die Verwendung von IBM Forms Server zu konfigurieren. Zum Konfigurieren von IBM Forms Server sind sowohl der Parameter **webFormConfig** als auch der Parameter **webFormInstallRoot** erforderlich. Dieser Parameter ist nur für eigenständige Serverprofile gültig.

**Anmerkung:** Die Konfiguration von IBM Forms Server anhand dieser Parameter ist nur für lokale Installationen von IBM Forms Server gültig.

#### **-webServerCheck true | false**

Gibt an, ob Web-Server-Definitionen erstellt werden sollen. Die gültigen Werte lauten **true** und **false**. Der Standardwert für diesen Parameter lautet **false**. Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

#### **-webServerHostname hostname\_des\_web-servers**

Der Hostname des Servers. Der Standardwert für diesen Parameter ist die Langform des Hostnamens der lokalen Workstation. Verwenden Sie diesen Pa-



parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

**-webServerInstallPath** *installationspfadname\_des\_web-servers*

Der Installationspfad des Web-Servers (lokal oder fern). Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

Der Standardwert für diesen Parameter ist von dem Betriebssystem der lokalen Workstation und vom Wert für den Parameter **webServerType** abhängig. Dazu ein Beispiel: **AIX**

```
webServerType=IHS: webServerInstallPath defaulted to /usr/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n/a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
webServerType=DOMINO: webServerInstallPath defaulted to ?
webServerType=APACHE: webServerInstallPath defaulted to ?
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

**HP-UX**

```
webServerType=IHS: webServerInstallPath defaulted to /opt/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n/a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

**> Linux**

```
webServerType=IHS: webServerInstallPath defaulted to /opt/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n/a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

```
webServerType=IHS: webServerInstallPath defaulted to /opt/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n/a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

**> Windows**

```
webServerType=IHS: webServerInstallPath defaulted to C:\Program Files\IBM\HTTPServer
webServerType=IIS: webServerInstallPath defaulted to C:\
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to C:\
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

**-webServerName** *web-server\_name*

Der Name des Web-Servers. Der Standardwert dieses Parameters lautet `web-server1`. Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

**-webServerOS** *web-server\_betriebssystem*

Das Betriebssystem, in dem sich der Web-Server befindet. Die gültigen Werte lauten wie folgt: `windows`, `linux`, `solaris`, `aix`, `hpux`, `os390` und `os400`. Verwenden Sie diesen Parameter in Verbindung mit dem Parameter **webServerType**.

Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

**-webServerPluginPath** *web-server\_pluginpfad*

Der Pfad zu den Plug-ins, die vom Web-Server verwendet werden. Der Standardwert für diesen Parameter lautet *installationsstammverzeichnis/plugins*. Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

**-webServerPort** *web-server\_port*

Gibt den Port an, über den auf den Web-Server zugegriffen wird. Der Standardwert für diesen Parameter lautet 80. Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

**-webServerType** *web-server\_typ*

Der Typ des Web-Servers. Die gültigen Werte lauten wie folgt: IHS, SUNJAVA-SYSTEM, IIS, DOMINO, APACHE und HTTPSERVER\_ZOS. Verwenden Sie diesen Parameter in Verbindung mit dem Parameter **webServerOS**. Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

► Windows

**-winserviceAccountType** *specifieduser* | **localsystem**

Der Typ des Eignerkontos für den Windows-Dienst, der für dieses Profil erstellt wurde. Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

Die gültigen Werte lauten *specifieduser* und *localsystem*. Der Wert für *localsystem* führt den Windows-Dienst unter dem lokalen Konto des Benutzers aus, der das Profil erstellt. Der Standardwert für diesen Parameter lautet *system*.

► Windows

**-winserviceCheck** **true** | **false**

Der Wert kann entweder 'true' oder 'false' lauten. Geben Sie **true** an, um einen Windows-Dienst für den Serverprozess zu erstellen, der innerhalb des Profils erstellt wird. Geben Sie **false** an, um den Windows-Dienst nicht zu erstellen. Der Standardwert für diesen Parameter lautet **false**.

Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

**-winservicePassword** *windienst\_kennwort*

Geben Sie das Kennwort für den angegebenen Benutzer oder das lokale Konto an, das als Eigner des Windows-Dienstes definiert werden soll. Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

► Windows

**-winserviceStartupType** **manual** | **automatic** | **disabled**

Die möglichen Werte für den Start des Windows-Dienstes lauten wie folgt:

- manual
- automatic
- disabled

Der Standardwert für diesen Parameter lautet `manual`.

Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

#### Windows

**-winserviceUserName** *windienst\_benutzer-id*

Geben Sie Ihre Benutzer-ID an, sodass das Windows-Betriebssystem überprüfen kann, ob Ihre ID zur Erstellung eines Windows-Dienstes berechtigt ist. Ihre Benutzer-ID muss zur Administratorgruppe gehören und über die folgenden erweiterten Benutzerberechtigungen verfügen:

- Einsetzen als Teil des Betriebssystems
- Anmelden als Dienst

Der Standardwert für diesen Parameter ist der aktuelle Benutzername. Der Wert für diesen Parameter darf weder Leerzeichen noch die folgenden ungültigen Zeichen enthalten: \*, ?, ", <, >, ,, /, \ und |. Der Benutzer, den Sie angeben, muss über die erforderlichen Berechtigungen zum Erstellen eines Windows-Dienstes verfügen. Sie müssen das korrekte Kennwort für den Benutzernamen angeben, der von Ihnen ausgewählt wurde.

Verwenden Sie diesen Parameter nur bei der Verwendung von Profilen. Geben Sie diesen Parameter nicht an, wenn Sie ein vorhandenes Profil erweitern.

## Business Space im Assistenten für die Konfiguration der Implementierungsumgebung konfigurieren

Der Assistent für die Konfiguration der Implementierungsumgebung führt die Konfiguration von Business Space und die Konfiguration von REST-Services für Widgets in Business Space automatisch durch. Sie können dabei festlegen, welcher REST-Service konfiguriert werden soll.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Installieren Sie Ihr Produkt.
- Erstellen Sie ein Profil. Achten Sie dabei darauf, den vollständig qualifizierten Hostnamen für das Profil anzugeben.
- Aktivieren Sie die Sicherheit, wenn Sie für Business Space eine gesicherte Umgebung einrichten wollen.

Wenn Sie Deployment Manager-Profilen und benutzerdefinierte Profile einrichten, ist dies die einfachste Methode zum Konfigurieren von Business Space.

1. Klicken Sie in der Administrationskonsole auf **Server > Implementierungsumgebungen > Neu**. Über eine Reihe von Seiten in dem Assistenten werden Sie durch die Erstellung Ihrer Implementierungsumgebung geführt.
2. Sie können die neue Implementierungsumgebung entweder definieren oder eine Datei importieren, die Definitionen für Implementierungsumgebungen enthält. Sie können eine Implementierungsumgebung auf Basis einer der von IBM bereitgestellten Muster erstellen oder eine angepasste Implementierungsumgebung erstellen.
3. Wählen Sie auf der Seite '**Muster für Implementierungsumgebung**' eines der Muster für die Implementierungsumgebung aus.
4. Legen Sie auf der Seite '**Knoten auswählen**' die Knoten fest, die in Ihre Implementierungsumgebung eingebunden werden sollen.

5. Geben Sie auf der Seite '**Cluster**' die Anzahl der Cluster-Member der einzelnen Knoten an, denen spezielle Funktionen der Implementierungsumgebung zugeordnet werden sollen.
6. Konfigurieren Sie auf der Seite '**Datenbank**' die Datenquelle für Business Space, wobei eine der in der Tabelle aufgelisteten Komponenten verwendet werden sollte. Sie können die Beschreibung bearbeiten, die Verbindung testen und das Datenbankprodukt festlegen, das für den Provider verwendet werden soll. Wenn die Business Space-Tabellen automatisch erstellt und konfiguriert werden sollen, markieren Sie das Kontrollkästchen **Tabellen erstellen**. Wenn Sie das Kontrollkästchen nicht auswählen, müssen Sie die Datenbank manuell für Business Space konfigurieren. Die Liste der Datenbankprodukte enthält alle Datenbanken, die von den einzelnen Komponenten unterstützt werden.

**Tipp:** Wenn Sie das Kontrollkästchen **Tabellen erstellen** auswählen, vergewissern Sie sich, dass vorher die Datenbank generiert wurde, bevor die Implementierungsumgebung erstellt wird.

7. Konfigurieren Sie auf der Seite **Sicherheit** die Authentifizierungsaliasnamen, die WebSphere für den Zugriff auf sichere Komponenten verwendet. Der Benutzername und das Kennwort für Authentifizierungsaliasnamen können auf dieser Seite geändert werden. Diese Aliasnamen ermöglichen den Zugriff auf geschützte Komponenten, jedoch nicht den Zugriff auf Datenquellen.
8. Für die IBM Business Process Manager-Konfiguration müssen Sie die zum Konfigurieren des Anwendungsimplementierungsziels für die Unterstützung der Implementierung von Business Process Choreographer-Komponenten erforderlichen Informationen angeben. Geben Sie die Stammkontexte, Sicherheitseinstellungen und die Werte für die Human Task Manager-Mailsitzung an, die vom Assistenten zum Konfigurieren von Business Process Choreographer für diese Implementierungsumgebung verwendet werden.
9. Konfigurieren Sie für die Konfiguration von IBM Business Process Manager den Business Process Rules Manager für die Ausführung in dem Cluster oder auf dem Server.
10. Konfigurieren Sie auf der Seite **REST-Services** die Services für die Widgets, die in Business Space für die Laufzeitumgebung bereitgestellt werden sollen.
  - Geben Sie die Portnummer und den Host bzw. virtuellen Host ein, der von einem Client zur Kommunikation mit dem Server oder Cluster benötigt wird. In einer Clusterumgebung ist dies in der Regel der Hostname und Port des Lastausgleichsservers.
  - Wenn Sie im Feld für den Host und den Port keine Angaben machen, dann werden dort standardmäßig die Werte eines einzelnen Cluster-Member-Hosts und des zugehörigen HTTP-Ports verwendet. Für eine Lastausgleichsumgebung müssen Sie die Standardwerte anschließend ändern und stattdessen den Namen des virtuellen Hosts und des Ports Ihres Lastausgleichsservers angeben. Achten Sie darauf, den vollständig qualifizierten Hostnamen anzugeben.
  - Definieren Sie die Beschreibung für Widgets, sofern dies erforderlich ist.
11. Klicken Sie auf der nächsten Seite auf **Fertig stellen** oder **Fertig stellen und Umgebung generieren**.
12. Optional: Wenn Sie das Kontrollkästchen **Tabellen erstellen** auf der Seite **Datenbank** nicht markiert hatten, führen Sie die Scripts zum Konfigurieren der Datenbanktabellen für Business Space aus, bevor Sie die Implementierungsumgebung oder die Cluster starten. Weitere Informationen hierzu finden Sie im Abschnitt Business Space-Datenbank konfigurieren.

**Tipp:** Business Space verwendet eine Proxy-Serverkomponente, um eine Verbindung zu Ihren REST-Services herzustellen. Falls die REST-Services nicht immer reagieren, müssen Sie die Einstellungen für das Verbindungszeitlimit zwischen Business Space und Ihren REST-Services aktualisieren, je nachdem, wie die Leistung auf den Servern für die REST-Services ist. Weitere Informationen enthält der Abschnitt Einstellung für die Zeitlimitüberschreitung für den Business Space-Ajax-Proxy-Server ändern.

## **Business Space für Network Deployment-Umgebungen konfigurieren**

Konfigurieren Sie Business Space in einer verteilten oder Network Deployment-Umgebung über die Administrationskonsole oder mithilfe von Befehlen.

Wenn Sie Deployment Manager- und benutzerdefinierte Profile benutzen, müssen Sie die REST-Endpunkte konfigurieren, Business Space konfigurieren, die REST-Endpunkte registrieren und die Datenbanktabellen konfigurieren.

### **REST-Services konfigurieren:**

Wenn Sie eine eigenständige Serverumgebung haben oder die Laufzeitumgebung mit dem Assistenten für die Implementierungsumgebung konfigurieren, werden die REST-Services automatisch konfiguriert und aktiviert. Konfigurieren Sie die REST-Services in anderen Umgebungen über die Administrationskonsole.

Wenn Widgets in Business Space verfügbar sein sollen, müssen Sie die REST-Services für diese Widgets konfigurieren. Später müssen Sie die REST-Endpunkte registrieren, damit Business Space die Widgets den Endpunkten zuordnet und die Widgets in der Palette zur Verwendung angezeigt werden.

Sie können alle REST-Services für einen bestimmten Server oder Cluster konfigurieren. Alternativ können Sie einzelne Services zum Konfigurieren auswählen. Sie können die Konfiguration einzelner Services verwalten, indem Sie alle Services für einen Service-Provider oder alle Services für Ihre Umgebung anzeigen.

REST-Services werden in der Regel auf dem REST-Gateway zugänglich gemacht. Einige REST-Services werden von ihrer dedizierten Systemanwendung implementiert. Die REST-Service-Gateway-Anwendung aktiviert allgemeine System-REST-Services. Diese Anwendung wird erstellt, wenn die REST-Services konfiguriert werden.

In Clusterumgebungen werden sämtliche Administrations- und Konfigurations-tasks für REST-Services in der Dmgr-Anwendung auf dem REST-Service-Gateway auf dem Deployment Manager ausgeführt. Die Dmgr-Anwendung auf dem REST-Service-Gateway wird mit den folgenden Widgets verwendet:

- Modulbrowser
- Modul-Assembly
- Moduleigenschaften
- Proxy-Gateway
- Modulzustand
- Systemzustand

*Alle REST-Services in der Administrationskonsole konfigurieren:*

Auf der Seite der Administrationskonsole für REST-Services können Sie alle REST-Services für Ihre Umgebung konfigurieren.

Vor der Ausführung dieser Task müssen Sie Ihr IBM Geschäftsprozessmanagementprodukt installieren.

Die Implementierung der REST-Services wird in einem eigenständigen Serverprofil automatisch ausgeführt. Für andere Konfigurationstypen können Sie auf der Seite der Administrationskonsole die REST-Services für alle Widgets Ihres Produkts in Business Space konfigurieren. Auf der Seite 'REST-Services' können Sie alle Services für Ihre Umgebung anzeigen und die einzelnen Services aktivieren oder inaktivieren.

Sie müssen auch die REST-Endpunkte bei Business Space registrieren. Anschließend ordnet Business Space diesen Endpunkten Widgets zu und die Widgets werden zur Verwendung in der Palette angezeigt. Stellen Sie wie im Abschnitt Mit der Administrationskonsole Business Space konfigurieren und REST-Endpunkte registrieren beschrieben sicher, dass die REST-Endpunkte bei Business Space registriert sind.

Wenn Sie mehrere Instanzen des gleichen REST-Serviceendpunkts konfigurieren wollen, müssen Sie die Endpunktdatei und die Widgetmetadatendatei manuell bearbeiten. Weitere Informationen hierzu finden Sie im Abschnitt Business Space-Widgets für die Verwendung mehrerer Endpunkte aktivieren.

Die REST-Service-Gateway-Anwendung aktiviert allgemeine System-REST-Services. Diese Anwendung wird erstellt, wenn die REST-Services konfiguriert werden.

1. Klicken Sie auf **Services > REST-Services > REST-Services**.

Die Seite 'REST-Services' wird geöffnet und zeigt alle REST-Services in Ihrer Umgebung an.

2. Geben Sie im Abschnitt **Geltungsbereich** die Option 'Alle' an, um sämtliche REST-Services in Ihrer Umgebung anzuzeigen, oder wählen Sie einen Server oder Cluster aus, auf bzw. in dem Sie REST-Services aktiviert haben. Wenn REST-Services, die Sie im ausgewählten Geltungsbereich erwartet hätten, nicht angezeigt werden, müssen Sie das REST-Service-Gateway oder die zugehörigen REST-Service-Provider auf dem Server bzw. in dem Cluster aktivieren. Siehe dazu REST-Services für Server, Cluster oder Komponenten konfigurieren.

3. Aktivieren Sie in den einzelnen Zeilen der Tabelle mit den REST-Services des Providers das Kontrollkästchen **Aktiviert**, um den entsprechenden REST-Service zu aktivieren, oder inaktivieren Sie das Kontrollkästchen **Aktiviert**, um den entsprechenden REST-Service zu inaktivieren.

4. Geben Sie für jeden Service, den Sie aktivieren wollen, in der Spalte **Beschreibung** eine aussagekräftige Beschreibung ein.

5. Klicken Sie auf **OK**, um die Änderungen in den Services festzuschreiben.

- Konfigurieren Sie Business Space.
- Konfigurieren Sie die Datenbanktabellen (bei Verwendung einer fernen Datenbank oder einer Network Deployment-Umgebung).
- Registrieren Sie die REST-Serviceendpunkte.
- Für mehrere Instanzen von Serviceendpunkten müssen Sie die zusätzlichen Widgets für jeden zusätzlichen Cluster manuell aktivieren. Dies kann beispielsweise der Fall sein, wenn Sie Ihren vorhandenen Workload auf zwei Cluster aufteilen (partitionieren) wollen und wenn die Widgets die Daten nach Clustern unterteilt anzeigen sollen.
- Konfigurieren Sie die Sicherheitsfunktion für Business Space.

*REST-Services in einem Service-Provider konfigurieren:*



Auf der Seite der Administrationskonsole für die Konfiguration der REST-Service-Provider können Sie die REST-Services in einem Service-Provider konfigurieren.

Vor der Ausführung dieser Task müssen Sie Ihr IBM Geschäftsprozessmanagementprodukt installieren.

Die Implementierung der REST-Services wird in einem eigenständigen Serverprofil automatisch ausgeführt. Für andere Konfigurationstypen können Sie in der Administrationskonsole die REST-Services für alle Widgets Ihres Produkts in Business Space konfigurieren. Auf der Seite der Administrationskonsole für die Konfiguration der REST-Service-Provider können Sie alle Services für einen ausgewählten Service-Provider anzeigen und die einzelnen Services aktivieren oder inaktivieren. Auf dieser Seite können Sie die Konfiguration einzelner Services verwalten, indem Sie alle Services für einen Service-Provider verwenden.

Sie müssen auch die REST-Endpunkte bei Business Space registrieren. Anschließend ordnet Business Space diesen Endpunkten Widgets zu und die Widgets werden zur Verwendung in der Palette angezeigt. Stellen Sie wie im Abschnitt Mit der Administrationskonsole Business Space konfigurieren und REST-Endpunkte registrieren beschrieben sicher, dass die REST-Endpunkte bei Business Space registriert sind.

Wenn Sie mehrere Instanzen des gleichen REST-Serviceendpunkts konfigurieren wollen, müssen Sie die Endpunktdatei und die Widgetmetadatendatei manuell bearbeiten. Weitere Informationen hierzu finden Sie im Abschnitt Business Space-Widgets für die Verwendung mehrerer Endpunkte aktivieren.

Die REST-Service-Gateway-Anwendung aktiviert allgemeine System-REST-Services. Diese Anwendung wird erstellt, wenn die REST-Services konfiguriert werden.

Die folgenden REST-Service-Provider sind verfügbar und werden im angegebenen Geltungsbereich definiert:

- **REST-Service-Gateway:** Um ein REST-Service-Gateway für einen bestimmten Geltungsbereich hinzuzufügen, wechseln Sie zu **Server > Servertypen > servername > Business Integration > REST-Services** oder **Server > Cluster > clustername > Business Integration > REST-Services**. Konfigurieren Sie den REST-Service-Gateway-Provider für den gegebenen Server oder Cluster.
  - **REST-Services-Gateway-Dmgr:** Der REST-Service-Gateway-Provider auf dem Deployment Manager wird automatisch konfiguriert, wenn Sie ein IBM Business Process Manager- oder WebSphere Enterprise Service Bus-Deployment Manager-Profil erstellen. Dieser Provider umfasst administrative REST-Services, die von den Widgets 'Modulbrowser', 'Modulverwaltung', 'Diagnosemonitor' und 'Proxy-Gateway' verwendet werden.
1. Klicken Sie auf **Services > REST-Services > REST-Service-Provider** .  
Die Seite 'REST-Service-Provider' wird geöffnet und alle REST-Service-Provider werden angezeigt.
  2. Klicken Sie auf den Link eines Providers, um die Services für die Gruppe der von diesem Provider verwalteten REST-Services zu konfigurieren.  
Die Seite für die Konfiguration der REST-Service-Provider wird geöffnet und zeigt alle REST-Services in dem Provider an.
  3. Wählen Sie in der Liste ein **Protokoll** für alle REST-Services aus, die Sie konfigurieren wollen, sodass diese in Business Space verfügbar sind. Konfigurieren Sie einen vollständigen URL-Pfad, indem Sie entweder **https://** oder **http://** auswählen und dann einen Wert für **Hostname oder virtueller Host in einer**

**Lastausgleichsumgebung** und **Port** in die entsprechenden Felder eingeben. Verwenden Sie einen vollständig qualifizierten Hostnamen.

Falls Sie möchten, dass REST-Anforderungen direkt an den Anwendungsserver geleitet werden, geben Sie den Hostnamen und den Port des Anwendungsservers ein. Falls die REST-Anforderungen an einen Proxy-Server oder einen HTTP-Server geleitet werden sollen, der sich vor einem oder mehreren Anwendungsservern befindet, geben Sie den Hostnamen und den Port des Proxy-Servers oder des HTTP-Servers ein, den Sie bereits eingerichtet haben. Stellen Sie in einer Umgebung mit einer Einrichtung für den Lastausgleich oder einem Proxy-Server zwischen Browser sowie Business Space und REST-Service sicher, dass das, was Sie für Protokoll, Host und Port festlegen, der Browser-URL für den Zugriff auf Business Space entspricht.

4. Aktivieren Sie in den einzelnen Zeilen der Tabelle mit den REST-Services des Providers das Kontrollkästchen **Aktiviert**, um den entsprechenden REST-Service zu aktivieren, oder inaktivieren Sie das Kontrollkästchen **Aktiviert**, um den entsprechenden REST-Service zu inaktivieren.
5. Geben Sie für jeden Service, den Sie aktivieren wollen, in der Spalte **Beschreibung** eine aussagekräftige Beschreibung ein.
6. Klicken Sie auf **OK**, um die Änderungen in den Services festzuschreiben.
  - Konfigurieren Sie Business Space.
  - Konfigurieren Sie die Datenbanktabellen (bei Verwendung einer fernen Datenbank oder einer Network Deployment-Umgebung).
  - Registrieren Sie die REST-Serviceendpunkte.
  - Für mehrere Instanzen von Serviceendpunkten müssen Sie die zusätzlichen Widgets für jeden zusätzlichen Cluster manuell aktivieren. Dies kann beispielsweise der Fall sein, wenn Sie Ihren vorhandenen Workload auf zwei Cluster aufteilen (partitionieren) wollen und wenn die Widgets die Daten nach Clustern unterteilt anzeigen sollen.
  - Konfigurieren Sie die Sicherheitsfunktion für Business Space.

*REST-Services für einen Server, Cluster oder eine Komponente konfigurieren:*

Auf der Seite der Administrationskonsole für REST-Services können Sie die REST-Services für einen Server, Cluster oder eine Komponente konfigurieren.

Vor der Ausführung dieser Task müssen Sie Ihr IBM Geschäftsprozessmanagementprodukt installieren.

Die Implementierung der REST-Services wird in einem eigenständigen Serverprofil automatisch ausgeführt. Für andere Konfigurationstypen können Sie auf der Seite der Administrationskonsole für REST-Services die Services für einen Server, Cluster oder eine Komponente konfigurieren.

Diese Task konfiguriert die REST-Service-Provider-Anwendung für einen bestimmten Server oder Cluster. Sie müssen die Provider-Anwendung konfigurieren, damit die REST-Services auf einem Server oder in einem Cluster zur Verfügung stehen. Weitere Informationen zu REST-Service-Providern finden Sie im Abschnitt REST-Services in einem Service-Provider konfigurieren.

Sie müssen auch die REST-Endpunkte bei Business Space registrieren. Anschließend ordnet Business Space diesen Endpunkten Widgets zu und die Widgets werden zur Verwendung in der Palette angezeigt. Stellen Sie wie im Abschnitt Mit der

Administrationskonsole Business Space konfigurieren und REST-Endpunkte registrieren beschrieben sicher, dass die REST-Endpunkte bei Business Space registriert sind.

Wenn Sie mehrere Instanzen des gleichen REST-Serviceendpunkts konfigurieren wollen, müssen Sie die Endpunktdatei und die Widgetmetadatendatei manuell bearbeiten. Weitere Informationen hierzu finden Sie im Abschnitt "Business Space-Widgets für die Verwendung mehrerer Endpunkte aktivieren".

Die REST-Service-Gateway-Anwendung aktiviert allgemeine System-REST-Services. Diese Anwendung wird erstellt, wenn die REST-Services konfiguriert werden.

1. Klicken Sie auf eine der folgenden Optionsfolgen.

- Für REST-Services auf einem Server: **Server > Servertypen > WebSphere-Anwendungsserver > name\_des\_servers > Business Integration > REST-Services.**
- Für REST-Services auf einem Cluster: **Server > Cluster > WebSphere-Anwendungsservercluster > name\_des\_clusters > Business Integration > REST-Services.**

Daraufhin wird die Seite 'REST-Services' aufgerufen, auf der alle REST-Services angezeigt werden, die Sie für Business Space-Widgets zur Verwendung in Ihrem Produkt oder Ihrer Komponente (Business Flow Manager oder Human Task Manager) konfigurieren können. Wenn bereits ein REST-Service konfiguriert wurde, wird eine entsprechende Nachricht angezeigt.

2. Wählen Sie in der Liste ein **Protokoll** für alle REST-Services aus, die Sie konfigurieren wollen, sodass diese in Business Space verfügbar sind. Konfigurieren Sie einen vollständigen URL-Pfad, indem Sie entweder **https://** oder **http://** auswählen und dann einen Wert für **Hostname oder virtueller Host in einer Lastausgleichsumgebung** und **Port** in die entsprechenden Felder eingeben. Verwenden Sie einen vollständig qualifizierten Hostnamen.

Falls Sie möchten, dass REST-Anforderungen direkt an den Anwendungsserver geleitet werden, geben Sie den Hostnamen und den Port des Anwendungsservers ein. Falls die REST-Anforderungen an einen Proxy-Server oder einen HTTP-Server geleitet werden sollen, der sich vor einem oder mehreren Anwendungsservern befindet, geben Sie den Hostnamen und den Port des Proxy-Servers oder des HTTP-Servers ein, den Sie bereits eingerichtet haben. Stellen Sie in einer Umgebung mit einer Einrichtung für den Lastausgleich oder einem Proxy-Server zwischen Browser sowie Business Space und REST-Service sicher, dass das, was Sie für Protokoll, Host und Port festlegen, der Browser-URL für den Zugriff auf Business Space entspricht. Dieselbe Einschränkung gilt für alle Umgebungen, die Flex-fähige Business Space-Widgets verwenden.

3. Aktivieren Sie in den einzelnen Zeilen der Tabelle mit den REST-Services das Kontrollkästchen **Aktiviert**, um den entsprechenden REST-Service zu aktivieren, oder inaktivieren Sie das Kontrollkästchen **Aktiviert**, um den entsprechenden REST-Service zu inaktivieren.

4. Geben Sie in der Tabelle der REST-Services im Feld **Beschreibung** eine aussagekräftige Beschreibung für alle REST-Services ein.

5. Klicken Sie auf **OK**, um die Änderungen in den Services festzuschreiben.

Wenn Sie später die Konfiguration der REST-Services ändern wollen, können Sie zu der Seite 'REST-Services' zurückkehren oder auf anderen Seiten der Administrationskonsole die Konfiguration der REST-Serviceendpunkte verwalten. Auf der Seite für die REST-Service-Provider können Sie Service-Provider für die

Konfiguration auswählen. Wenn Sie über **Services > REST-Services** auf die Seite 'REST-Services' zugreifen, können Sie alle REST-Services in Ihrer Umgebung konfigurieren.

- Konfigurieren Sie Business Space.
- Konfigurieren Sie die Datenbanktabellen (bei Verwendung einer fernen Datenbank oder einer Network Deployment-Umgebung).
- Registrieren Sie die REST-Serviceendpunkte.
- Für mehrere Instanzen von Serviceendpunkten müssen Sie die zusätzlichen Widgets für jeden zusätzlichen Cluster manuell aktivieren. Dies kann beispielsweise der Fall sein, wenn Sie Ihren vorhandenen Workload auf zwei Cluster aufteilen (partitionieren) wollen und wenn die Widgets die Daten nach Clustern unterteilt anzeigen sollen.
- Konfigurieren Sie die Sicherheitsfunktion für Business Space.

*REST-Services über die Befehlszeile konfigurieren:*

Alle für Ihr Produkt erforderlichen Widgets werden mit Business Space powered by WebSphere installiert. Die REST-Services (REST = Representational State Transfer) für Widgets müssen in Business Space konfiguriert, aktiviert und registriert werden, bevor Ihr Team die Widgets in Business Space verwenden kann. Wenn Sie nicht die Seite der Administrationskonsole für REST-Services verwenden, können Sie den Befehl **updateRESTGatewayService** verwenden.

Vor der Ausführung dieser Task müssen Sie Ihr IBM Geschäftsprozessmanagementprodukt installieren.

Die Implementierung der REST-Services wird in einem eigenständigen Serverprofil automatisch ausgeführt. Für andere Konfigurationstypen können Sie auf der Seite der Administrationskonsole für REST-Services oder mit dem Befehl **updateRESTGatewayService** die Services für REST-APIs für alle Widgets Ihres Produkts in Business Space konfigurieren.

Sie müssen auch die REST-Endpunkte bei Business Space registrieren. Anschließend ordnet Business Space diesen Endpunkten Widgets zu und die Widgets werden zur Verwendung in der Palette angezeigt.

Wenn Sie mehrere Instanzen des gleichen REST-Serviceendpunkts konfigurieren wollen, müssen Sie die Endpunktdatei und die Widgetmetadatendatei manuell bearbeiten. Weitere Informationen hierzu finden Sie im Abschnitt "Business Space-Widgets für die Verwendung mehrerer Endpunkte aktivieren".

1. Öffnen Sie ein Befehlsfenster.  
Der Befehl 'wsadmin' befindet sich in einer eigenständigen Serverumgebung im Verzeichnis *stammverzeichnis\_des\_profils/bin* und in einer Network Deployment-Umgebung im Verzeichnis *stammverzeichnis\_des\_deployment\_manager\_profils/bin*.
2. Geben Sie an der Eingabeaufforderung **wsadmin** ein, um die **wsadmin**-Umgebung zu starten.
3. Konfigurieren Sie die REST-Services mit dem Befehl **updateRESTGatewayService**. Geben Sie dabei den Cluster oder Server und den Knoten an. Der Parameter **-enable** ist optional. Wenn er nicht angegeben wird, nimmt er standardmäßig den Wert true (wahr) an.
4. Führen Sie den Befehl 'save' aus.

Im folgenden Beispiel wird mit Jython der Befehl **updateRESTGatewayService** ausgeführt. Anschließend werden die Änderungen gespeichert. Er konfiguriert die REST-Services in einem Cluster.

```
AdminTask.updateRESTGatewayService(['-clusterName  
  clustername'])  
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updateRESTGatewayService {-clusterName  
  clustername}  
$AdminConfig save
```

- Konfigurieren Sie Business Space.
- Konfigurieren Sie die Datenbanktabellen (bei Verwendung einer fernen Datenbank oder einer Network Deployment-Umgebung).
- Registrieren Sie die REST-Serviceendpunkte.
- Für mehrere Instanzen von Serviceendpunkten müssen Sie die zusätzlichen Widgets für jeden zusätzlichen Cluster manuell aktivieren. Dies kann beispielsweise der Fall sein, wenn Sie Ihren vorhandenen Workload auf zwei Cluster aufteilen (partitionieren) wollen und wenn die Widgets die Daten nach Clustern unterteilt anzeigen sollen.
- Konfigurieren Sie die Sicherheitsfunktion für Business Space.

### **In der Administrationskonsole Business Space konfigurieren und REST-Endpunkte registrieren:**

Sie können Business Space powered by WebSphere über die Administrationskonsole installieren und konfigurieren.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Installieren Sie die Software des Produkts und erstellen Sie ein Profil. Bei der Installation Ihres Produkts werden Business Space-Dateien für die von Ihnen definierten Profile in die Installation eingebunden. Ihr Profil wird erst für Business Space konfiguriert, wenn Sie Business Space explizit für das Profil konfigurieren.
- Aktivieren Sie die Sicherheit, wenn Sie für Business Space eine gesicherte Umgebung einrichten wollen.
- Konfigurieren Sie REST-Services. Wenn Sie eine eigenständige Serverumgebung haben oder die Laufzeitumgebung mit dem Assistenten für die Implementierungsumgebung konfigurieren, werden die REST-Serviceendpunkte automatisch konfiguriert und aktiviert. Konfigurieren Sie die REST-Services in anderen Umgebungen über die Seite der Administrationskonsole für REST-Services. Wenn Widgets in Business Space verfügbar sein sollen, müssen Sie die REST-Services für diese Widgets konfigurieren. Registrieren Sie die REST-Endpunkte auf der Seite 'Business Space - Konfiguration' der Administrationskonsole, damit Business Space die Widgets den Endpunkten zuordnet und die Widgets in der Palette zur Verwendung angezeigt werden.
- Wenn Sie Business Space mit einer anderen Datenquelle als der Produktdatenquelle auf einem Server oder in einem Cluster konfigurieren wollen, müssen Sie die Datenquelle im Server- oder Clustergeltungsbereich mit dem korrekten JNDI-Namen jdbc/mashupDS erstellen, bevor Sie Business Space über die Administrationskonsole konfigurieren.
- Wenn Sie bei Oracle ein anderes als das von der Produktdatenbank verwendete Schema für die Business Space-Tabellen verwenden wollen, müssen Sie die folgenden Schritte ausführen, um manuell eine Datenquelle zu erstellen, bevor Sie die Seite 'Business Space - Konfiguration' öffnen:



1. Erstellen Sie das Schema über die Software des Datenbankprodukts.
2. JDBC-Provider über die Administrationskonsole konfigurieren.
3. Erstellen Sie über die Administrationskonsole die Datenquelle mit dem JNDI-Namen 'jdbc/mashupDS' je nach Ihrer Umgebung auf Server- oder Clusterebene.
4. Erstellen Sie über die Administrationskonsole einen Authentifizierungsalias. Legen Sie den Benutzernamen auf das erstellte Schema und die Authentifizierung entsprechend Ihrem Oracle-Setup fest.
5. Legen Sie den Authentifizierungsalias für die Datenquelle fest.

Wenn Sie mit Implementierungsumgebungen arbeiten oder andere erweiterte Profilkonfigurationen nutzen, müssen Sie die Administrationskonsole verwenden, um Business Space für den Einsatz in Ihrer Laufzeitumgebung zu konfigurieren. Business Space ist eine browserbasierte grafische Benutzerschnittstelle für Geschäftsbetreiber der Anwendung, die mit dem von Ihnen definierten Profil ausgeführt wird. In Business Space können Sie bzw. Ihre Benutzer den Inhalt von Produkten aus dem Portfolio von WebSphere Business Process Management anpassen.

1. Stellen Sie sicher, dass die Administrationskonsole ausgeführt wird.
2. Klicken Sie im Navigationsfenster auf **Server > Servertypen > WebSphere-Anwendungsserver** oder **Server > Cluster > WebSphere-Anwendungsserver-cluster**.
3. Wählen Sie den Namen Ihres Server- oder Clusterziels aus.
4. Klicken Sie auf der Seite 'Konfiguration' unter **Business Integration** auf **Business Space - Konfiguration**. Daraufhin wird die Seite 'Business Space - Konfiguration' geöffnet. Wenn Business Space bereits konfiguriert wurde, können Sie diese Seite zwar anzeigen, die Felder jedoch nicht bearbeiten.
5. Wählen Sie das Kontrollkästchen **Business Space-Service installieren** aus.
6. Geben Sie im Feld **Name des Datenbankschemas** den Namen des Datenbankschemas ein, das für die Business Space-Datenbank verwendet werden soll.

**Anmerkung:** In Oracle ist das Schema mit dem Benutzernamen identisch, der als Authentifizierungsalias für die Datenquelle festgelegt wird.

7. Wenn im Feld **Vorhandene Business Space-Datenquelle** keine Datenquelle angegeben ist, dann verwenden Sie **Business Space-Datenquelle erstellen mit** und wählen Sie eine Datenquelle aus, für die eine Verbindung zu der Datenbank hergestellt werden kann, die für Business Space verwendet werden soll.

Durch die Auswahl einer Datenquelle unter **Business Space-Datenquelle erstellen mit:** wird eine Datenquelle für Business Space mit dem JNDI-Namen jdbc/mashupDS erstellt, die anhand der von Ihnen ausgewählten Datenquelle modelliert wird.

Die Datenquelle für Business Space wird auf dem Server oder in dem Cluster erstellt, auf bzw. in dem Sie Business Space konfigurieren, selbst wenn sich die Produktdatenquelle auf einem anderen Server oder in einem anderen Cluster befindet.

**Tipp:** Wenn Sie keine der angezeigten Datenquellen verwenden wollen, dann müssen Sie die Seite 'Business Space - Konfiguration' schließen, die Datenbank sowie die zu verwendende Datenquelle einrichten und die Seite 'Business Space - Konfiguration' erneut aufrufen, um die Konfiguration durchzuführen. Weitere Informationen hierzu finden Sie im Abschnitt 'Vorbereitungen'.

8. Klicken Sie auf **OK**.



- Um das entsprechende Implementierungsziel (Cluster oder Server) für die REST-Serviceendpunkte der einzelnen Widgets zu registrieren, die Sie in Business Space verwenden, klicken Sie auf **REST-Serviceendpunkt - Registrierung**.

Das Ziel, das Sie für einen REST-Serviceendpunkttyp auswählen, kann den Geltungsbereich der in bestimmten Widgets angezeigten Daten definieren. Alternativ können Sie einen bestimmten Cluster oder Server auswählen, um eine bessere Leistung oder Verfügbarkeit zu erreichen.

Wenn Sie Widgets für die Benutzertaskverwaltung verwenden, können Sie in der Zeile für die Typen 'Prozessservices' und 'Task-Services' mehr als einen REST-Service-Provider für einen Server oder einen Cluster auswählen. Wählen Sie den Provider mit Name=Federated REST Services, den Provider mit Name=Business Process Choreographer REST Services oder den Provider mit Name=BPD Engine REST Services aus. Wenn Tasks und Prozesse sowohl in Business Process Choreographer als auch in der BPD-Engine (BPD = Business Process Definition) ausgeführt werden, wählen Sie die eingebundenen REST-Services aus. Wenn Sie nur Prozesse und Tasks verwenden, die in Business Process Choreographer (modelliert in Integration Designer) ausgeführt werden, wählen Sie die Business Process Choreographer-REST-Services aus. Wenn Sie nur Prozesse und Tasks verwenden, die in der BPD-Engine (modelliert in Process Designer) ausgeführt werden, wählen Sie die BPD-Engine aus.

Wenn Sie das Ziel nicht angeben, wird der REST-Endpunkt dieses Typs nicht bei Business Space registriert, und die Widgets, die den REST-Serviceendpunkt dieses Typs benötigen, werden in Business Space nicht angezeigt.

- Speichern Sie die Konfiguration.
- Führen Sie die Scripts zum Konfigurieren der Datenbanktabellen für Business Space aus, bevor Sie die Implementierungsumgebung oder die Cluster starten. Die Scripts wurden nach Abschluss der Konfiguration generiert. Weitere Informationen hierzu finden Sie im Abschnitt Business Space-Datenbank konfigurieren.

**Anmerkung:** Wenn Sie Oracle verwenden, wird das Kennwort für den Authentifizierungsalias der Business Space-Datenquelle mit dem Schemanamen von Business Space festgelegt. Der Standardwert für das Schema lautet IBMBUSSP. Wenn Sie Business Space konfigurieren, können Sie in der Administrationskonsole oder in der Befehlszeile auch ein anderes Schema angeben. In dem Fall lautet das Standardkennwort genauso wie das Schema, das Sie angeben. Wenn Sie ein anderes Kennwort für den Business Space-Benutzernamen festlegen möchten, müssen Sie über die Administrationskonsole die JDBC-Ressourcen aktualisieren: Suchen Sie die Datenquelle jdbc/mashupsDS. Ändern Sie den Wert für den Authentifizierungsalias so, dass er dem Kennwort des Business Space-Schemanamens entspricht. Speichern Sie Ihre Änderungen und starten Sie den Server erneut.

**Anmerkung:** Business Space verwendet eine Proxy-Serverkomponente, um eine Verbindung zu Ihren REST-Services herzustellen. Falls die REST-Services nicht immer reagieren, müssen Sie die Einstellungen für das Verbindungszeitlimit zwischen Business Space und Ihren REST-Services aktualisieren, je nachdem, wie die Leistung auf den Servern für die REST-Services ist. Weitere Informationen enthält der Abschnitt Einstellung für die Zeitlimitüberschreitung für den Business Space-Ajax-Proxy ändern.

**Business Space über die Befehlszeile konfigurieren:**

Business Space powered by WebSphere kann mit dem Befehl **wsadmin** installiert und konfiguriert werden. Mit dem Befehl **wsadmin** können Sie Business Space wie über die Administrationskonsole konfigurieren.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Installieren Sie die Software des Produkts und erstellen Sie ein Profil. Bei der Installation Ihres Produkts werden Business Space-Dateien für die von Ihnen definierten Profile in die Installation eingebunden. Ihr Profil wird erst für Business Space konfiguriert, wenn Sie Business Space explizit für das Profil konfigurieren.
- Wenn Sie für Business Space eine gesicherte Umgebung einrichten wollen, aktivieren Sie die Sicherheit.
- Wenn Sie beabsichtigen, eine Datenbankentwurfsdatei für die Business Space-Datenbankinformationen zu verwenden, führen Sie die Schritte in „Eigenschaftendatei für Business Space-Datenbankentwurf erstellen“ auf Seite 254 aus.
- Konfigurieren Sie REST-Services. Wenn Sie eine eigenständige Serverumgebung haben oder die Laufzeitumgebung mit dem Assistenten für die Implementierungsumgebung konfigurieren, werden die REST-Serviceendpunkte automatisch konfiguriert und aktiviert. Konfigurieren Sie die REST-Services in anderen Umgebungen über die Seite der Administrationskonsole für REST-Services. Wenn Widgets in Business Space verfügbar sein sollen, müssen Sie die REST-Serviceendpunkte für diese Widgets konfigurieren. Sie müssen die REST-Endpunkte registrieren, damit Business Space die Widgets den Endpunkten zuordnet und die Widgets in der Palette zur Verwendung angezeigt werden.
- Wenn Sie Business Space mit einer anderen Datenquelle als der Produktdatenquelle auf einem Server oder in einem Cluster konfigurieren wollen, müssen Sie die Datenquelle im Server- oder Clustergeltungsbereich mit dem korrekten JNDI-Namen `jdbc/mashupDS` erstellen, bevor Sie Business Space (durch Ausführung des Befehls **configureBusinessSpace**) konfigurieren.
- Wenn Sie bei Oracle ein anderes als das von der Produktdatenbank verwendete Schema für die Business Space-Tabellen verwenden wollen, müssen Sie die folgenden Schritte ausführen, um manuell eine Datenquelle zu erstellen, bevor Sie die Befehle für die Installation und Konfiguration von Business Space gemäß der folgenden Prozedur ausführen:
  - JDBC-Provider über die Administrationskonsole konfigurieren.
  - Erstellen Sie über die Administrationskonsole die Datenquelle mit dem JNDI-Namen `'jdbc/mashupDS'` je nach Ihrer Umgebung auf Server- oder Clusterebene.

Sie können die Befehlszeile verwenden, wenn Sie zum Konfigurieren von Business Space nicht die Administrationskonsole verwenden, sondern Scripts schreiben möchten.

Wenn Sie nicht sicher sind, ob Business Space bereits konfiguriert ist, können Sie mit dem Befehl **getBusinessSpaceDeployStatus** feststellen, ob Business Space für einen Server, einen Cluster oder eine Zelle konfiguriert ist. Weitere Informationen zu diesem Befehl finden Sie im Abschnitt "Befehl 'getBusinessSpaceDeployStatus'".

Führen Sie zum Konfigurieren von Business Space die folgenden Schritte aus.

1. Öffnen Sie ein Befehlsfenster.

Der Befehl `'wsadmin'` befindet sich in einer eigenständigen Serverumgebung im Verzeichnis `stammverzeichnis_des_profils/bin` und in einer Network Deployment-Umgebung im Verzeichnis `stammverzeichnis_des_deployment_manager_profils/bin`.

2. Geben Sie an der Eingabeaufforderung **wsadmin** ein, um die **wsadmin**-Umgebung zu starten.
3. Verwenden Sie den Befehl **installBusinessSpace**, um die EAR-Dateien für Business Space in der Laufzeitumgebung zu installieren.
4. Konfigurieren Sie die Datenquelle für Business Space mit dem Befehl **configureBusinessSpace** und kopieren Sie die Scripts, mit denen die Datenbanktabellen konfiguriert werden, für einen eigenständigen Server nach *installationsstammverzeichnis/dbscripts/BusinessSpace/knotenname\_servername/datenbanktyp/datenbankname* oder für einen Cluster nach *installationsstammverzeichnis/dbscripts/BusinessSpace/clustername/datenbanktyp/datenbankname*.

Wenn Sie bei der Ausführung des Befehls **configureBusinessSpace** für den Parameter **createTables** nicht wahr (true) angegeben haben, müssen Sie die Scripts ausführen, die die Datenbanktabellen konfigurieren. Weitere Informationen zu diesen Scripts finden Sie in „Business Space-Datenbank konfigurieren“ auf Seite 255.

Wenn Sie für die Datenbankkonfiguration eine Datenbankentwurfsdatei verwenden, können Sie diese Datei bei der Ausführung des Befehls **configureBusinessSpace** mit dem Parameter **-bspacedbDesign** angeben.

Stellen Sie bei der Verwendung einer Windows-Authentifizierung mit Microsoft SQL Server sicher, dass der Parameter **-dbWinAuth** als true gesetzt ist.

5. Führen Sie nach jedem Befehl `AdminConfig.save()` (mit Jython) oder `$AdminConfig save` (mit Jacl) aus.
6. Führen Sie die Scripts zum Konfigurieren der Datenbanktabellen für Business Space aus, bevor Sie die Implementierungsumgebung oder die Cluster starten. Weitere Informationen hierzu finden Sie im Abschnitt Business Space-Datenbanktabellen konfigurieren.

Durch die Konfiguration von Business Space wird eine browserbasierte grafische Benutzerschnittstelle für Geschäftsbenutzer Ihrer Anwendung eingerichtet, die mit dem von Ihnen definierten Profil ausgeführt wird. In Business Space können Sie bzw. Ihre Benutzer den Inhalt von Produkten aus dem Portfolio von WebSphere Business Process Management anpassen.

Im folgenden Beispiel werden mit Jython die Befehle **installBusinessSpace** und **configureBusinessSpace** ausgeführt, um in einem Cluster die EAR-Dateien zu installieren und die Datenquelle für Business Space zu konfigurieren. Bei der Installation mehrerer Produkte werden in dem Beispiel das Schema und die Produktdatenbank für Business Space angegeben. Wenn IBM Business Process Manager und IBM Business Monitor installiert werden, erstellt dieses Beispiel mithilfe der Eigenschaften der IBM Business Process Manager-Datenquelle eine Business Space-Datenquelle.

```
AdminTask.installBusinessSpace(['-clusterName myCluster -save true'])
AdminTask.configureBusinessSpace(['-clusterName myCluster -schemaName mySchema -productTypeForDatasource WPS -save true'])
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask installBusinessSpace {-clusterName myCluster -save true}
$AdminTask configureBusinessSpace {-clusterName myCluster -schemaName mySchema -productTypeForDatasource WPS -save true}
```

**Tipp:** Wenn Sie Oracle verwenden, wird das Kennwort für den Authentifizierungsaliasnamen der Business Space-Datenquelle auf denselben Wert wie der Schemaname von Business Space eingestellt. Der Standardwert für das Schema lautet IBM-BUSSP. Wenn Sie Business Space konfigurieren, können Sie in der Administrationskonsole oder in der Befehlszeile auch ein anderes Schema angeben. In dem Fall lautet das Standardkennwort genauso wie das Schema, das Sie angeben. Wenn Sie ein anderes Kennwort für den Business Space-Benutzernamen festlegen möchten, müssen Sie über die Administrationskonsole die JDBC-Ressourcen aktualisieren: Suchen Sie die Datenquelle jdbc/mashupsDS. Ändern Sie den Wert für den Authentifizierungsalias so, dass er dem Kennwort des Business Space-Schemanamens entspricht. Speichern Sie Ihre Änderungen und starten Sie den Server erneut.

Führen Sie nach der Konfiguration von Business Space die folgenden Schritte aus, um Business Space für Ihre Laufzeitumgebung zu aktivieren.

- Registrieren Sie die Endpunkte mit dem Befehl **registerRESTserviceEndpoint**.
- Richten Sie für Business Space und die von Ihrem Team verwendeten Widgets die benötigte Sicherheitsfunktion ein. Weitere Informationen hierzu finden Sie im Abschnitt zum Einrichten der Sicherheitsfunktion für Business Space.

**Tipp:** Business Space verwendet eine Proxy-Serverkomponente, um eine Verbindung zu Ihren REST-Services herzustellen. Falls die REST-Services nicht immer reagieren, müssen Sie die Einstellungen für das Verbindungszeitlimit zwischen Business Space und Ihren REST-Services aktualisieren, je nachdem, wie die Leistung auf den Servern für die REST-Services ist. Weitere Informationen enthält der Abschnitt Einstellung für die Zeitlimitüberschreitung für den Business Space-Ajax-Proxy ändern.

### **Eigenschaftendatei für Business Space-Datenbankentwurf erstellen:**

Wenn Ihr Business Space nicht den Standarddatenbanktyp verwendet, erstellen Sie eine Eigenschaftendatei für den Datenbankentwurf, um den Prozess der Datenbankerstellung zu vereinfachen.

Entwurfsdateischablonen für jeden Datenbanktyp sind im Verzeichnis *installationsstammverzeichnis/BusinessSpace/config.bspace/MetadataFiles* gespeichert; beispielsweise hat die Entwurfsdateischablone für DB2 folgenden Namen: BSpace\_DB2-distributed.properties.

1. Erstellen Sie eine neue Datei, indem Sie eine Kopie der Schablonendatei für Ihren Datenbanktyp erstellen.
2. Ändern Sie die Werte der eingestellten Eigenschaften in der Eigenschaftendatei für den Datenbankentwurf so, dass sie Ihrer Konfiguration entsprechen. Kommentare in der Datei helfen Ihnen, die richtigen Eigenschaftswerte zu wählen.

Geben Sie den vollständigen Pfad Ihrer Eigenschaftendatei für den Datenbankentwurf an einer der folgenden Positionen an (abhängig von Ihrer Produktumgebung und der bevorzugten Konfiguration):

- Wenn Sie das Profile Management Tool verwenden, um Business Space mit einem Profil zu konfigurieren, geben Sie die Datenbankentwurfsdatei an, indem Sie die Option **Datenbankentwurfsdatei verwenden** auswählen.
- Wenn Sie das Befehlszeilendienstprogramm **manageprofiles** verwenden, um Business Space mit einem Profil zu konfigurieren, geben Sie die Datenbankentwurfsdatei mit dem Parameter **-bspacedbDesign** an.

- Wenn Sie den Befehl **configureBusinessSpace** verwenden, um Business Space zu konfigurieren, geben Sie die Datenbankentwurfsdatei mit dem Parameter **-bspacedbDesign** an.

### Business Space-Datenbank konfigurieren:

Sie können Datenbanktabellen für Business Space auf einem fernen Datenbankserver manuell installieren, indem Sie Scripts verwenden, die vom Installationsprogramm generiert werden. Wenn Sie eine Implementierungsumgebung verwenden oder mit einer fernen Datenbank arbeiten, dann müssen Sie diese Tabellen installieren, nachdem Sie Business Space konfiguriert haben.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Installieren Sie das Produkt.
- Erstellen Sie die Profile und konfigurieren Sie die Server oder Cluster für Business Space.
- Für Oracle: Erstellen Sie die Datenbank.
- Für Microsoft SQL Server: Stellen Sie die Authentifizierung für die SQL Server-Instanz ein. Der SQL Server-JDBC-Treiber unterstützt nur den gemischten Authentifizierungsmodus. Daher muss die Authentifizierung bei der Erstellung der SQL Server-Instanz auf **SQL Server und Windows** eingestellt werden.
- Stellen Sie für alle Datenbanken sicher, dass die Datenbank mit dem Universalzeichensatz UTF-8 installiert wird, damit Sie Business Space in Ihrer Umgebung verwenden können.
- Stellen Sie sicher, dass Ihr Anwendungsserver mit Business Space gestoppt wird.

Wenn Sie DB2 for z/OS verwenden und die erforderlichen Ressourcen nicht bereits im Rahmen der Installation des Basisprodukts konfiguriert wurden, dann führen Sie die folgenden zusätzlichen Schritte aus, bevor Sie diese Task beginnen:

- Erstellen Sie eine TEMP-Datenbank sowie einen TEMP-Tabellenbereich, in der bzw. dem die deklarierten temporären Tabellen für die Verarbeitung verschiebbarer Cursor gespeichert werden sollen.
- Erstellen Sie eine dedizierte STOGROUP-Komponente, in der die Business Space-Daten gespeichert werden sollen.

Wenn Sie bei DB2 for z/OS eine andere Speichergruppe verwenden wollen (wenn beispielsweise Business Space-Datenbanktabellen nicht zu derselben Datenbank und Speichergruppe wie die Common-Datenbank hinzugefügt werden sollen), müssen Sie das Script `createTablespace_BusinessSpace.sql` bearbeiten und ausführen, nachdem Sie Business Space konfiguriert haben und bevor Sie die Business Space-Datenbanktabellen konfigurieren.

- Bearbeiten Sie die Datei `createTablespace_BusinessSpace.sql`, die sich an folgender Speicherposition befindet: `profilstammverzeichnis/dbscripts/BusinessSpace/knotenname_servername/datenbanktyp/datenbankname` (für einen eigenständigen Server) bzw. `profilstammverzeichnis/dbscripts/BusinessSpace/clustername/datenbanktyp/datenbankname` (für einen Cluster, wobei `datenbank` DB2zOS ist).
- Ändern Sie den Wert für VCAT von @VCAT@ in den Namen oder Aliasnamen des Katalogs der integrierten Katalogfunktion für die zu verwendende Speichergruppe.

Falls Sie DB2 V9.x verwenden und eine Leistungssteigerung erzielen möchten, bearbeiten Sie die Datei `createTablespace_BusinessSpace.sql`. Die Datei `createTablespace_BusinessSpace.sql` befindet sich an folgender Speicherposition:



*profilstammverzeichnis/dbscripts/BusinessSpace/knotenname\_servername/datenbanktyp/datenbankname* (für einen eigenständigen Server) bzw. *profilstammverzeichnis/dbscripts/BusinessSpace/clustername/datenbanktyp/datenbankname* (für einen Cluster).

- Ändern Sie IMMEDIATE SIZE 8000 PAGESIZE 32K in IMMEDIATE SIZE 8000 AUTOMATIC PAGESIZE 32K.
- Fügen Sie die Zeile PREFETCHSIZE AUTOMATIC nach EXTENTSIZE 16 sowohl unter CREATE SYSTEM TEMPORARY TABLESPACE @TSDIR@TMPTP als auch unter CREATE REGULAR TABLESPACE @TSDIR@REGTP hinzu.

Das Script configBusinessSpaceDB konfiguriert Tabellen für Business Space mit einer speziellen Datenbank. (Wenn Sie Tabellen in einer anderen vorhandenen Datenbank als der genannten erstellen wollen, müssen Sie mit Ihrem Produkt das Script createDBTables anstelle des Scripts configBusinessSpaceDB verwenden.)

Führen Sie zum Konfigurieren der Datenbanktabellen für Business Space die folgenden Schritte aus:

1. Stellen Sie sicher, dass Sie eine Benutzer-ID verwenden, deren Berechtigung für die Erstellung von Tabellen ausreicht.
2. Suchen Sie das Script in dem zuletzt konfigurierten Script und speichern Sie es unter einer Position auf demselben System, auf dem sich auch die Datenbank befindet.
  - Für alle Datenbanken außer DB2 for z/OS müssen Sie das Script configBusinessSpaceDB.bat oder configBusinessSpaceDB.sh suchen.
  - Für DB2 for z/OS müssen Sie die Business Space-Dateien individuell ausführen, wenn Sie das Script createDB.sh nicht ausführen. Suchen Sie nach createTablespace\_BusinessSpace.sql und createTable\_BusinessSpace.sql.

Standardmäßig befinden sich die Scripts im folgenden Verzeichnis:

*installationsstammverzeichnis/dbscripts/BusinessSpace/knotenname\_servername/datenbanktyp/datenbankname* (für einen eigenständigen Server) bzw. *installationsstammverzeichnis/dbscripts/BusinessSpace/clustername/datenbanktyp/datenbankname* (für einen Cluster). Die aktualisierten Scripts (mit den Angaben, die Sie bei der Profilerstellung eingegeben haben) befinden sich in dem Profil für den Server oder Cluster, den Sie zuletzt konfiguriert haben. Wenn Sie den Assistenten für die Konfiguration der Implementierungsumgebung verwendet haben, dann befinden sich die Scripts im Deployment Manager-Profil. Wenn Sie eine ferne Datenbank konfigurieren, dann kopieren Sie die Scripts von dem System, auf dem Ihr Produkt installiert ist, an eine Position auf dem fernen System.

3. Öffnen Sie eine Eingabeaufforderung und führen Sie danach abhängig vom verwendeten Betriebssystem einen der folgenden Befehle aus.

Kopieren Sie den Ordner mit den Batchdateien und Scripts an dieselbe Position wie Ihre Datenbank und führen Sie den Befehl dort aus. Ihre Benutzer-ID muss Zugriff auf den Befehlszeileninterpreter für den Datenbanktyp haben sowie über die Berechtigung verfügen, Befehle auszuführen.

-   configBusinessSpaceDB.sh
-  configBusinessSpaceDB.bat

Verwenden Sie bei DB2 und SQL Server den optionalen Parameter **-createDB**, wenn Sie anstelle der vorhandenen Datenbank eine andere Datenbank verwenden wollen.



**Einschränkung:** Wenn Sie SQL Server verwenden, werden Ihnen die folgenden Warnmeldungen in der Datei `systemout.log` nach der Ausführung des Datenbankskripts angezeigt: ... Warning! The maximum key length is 900 bytes ... Wenn Sie die eingebundenen Repositorys als eine Benutzerregistry verwenden, können Sie die Warnungen ignorieren. Wenn Sie die eigenständige LDAP-Registry verwenden, stellen Sie sicher, dass die Zahl der Zeichen in allen Einträgen für die registrierten Namen der Benutzer in Ihrem Unternehmen nicht die Zeichenbegrenzung von 131 überschreitet. Sollte die Zeichenzahl in einem der Benutzer-DN-Einträge den Wert von 131 Zeichen überschreiten, müssen Sie die Benutzerkontoregistry in die Option für eingebundene Repositorys ändern. Führen Sie für DB2 for z/OS die folgenden Dateien nacheinander aus:

- `createTablespace_BusinessSpace.sql`
- `createTable_BusinessSpace.sql`

4.    Für DB2 und DB2 for z/OS müssen Sie eine Bindung zwischen der Befehlszeilenschnittstelle und der Business Space-Datenbank herstellen, indem Sie die folgenden Befehle eingeben:

```
db2 connect to datenbankname
db2 bind DB2_installationsverzeichnis\bnd\@db2cli.lst blocking all
grant public
db2 connect reset
```

Dabei gilt Folgendes:

*datenbankname* ist der Name der Business Space-Datenbank.

*DB2\_installationsverzeichnis* ist das Verzeichnis, in dem DB2 installiert ist.

5. Wenn Sie die Business Space-Datenbank erneut erstellen, nachdem sie zuvor gelöscht wurde, müssen Sie die Business Space-Vorlagen und -Spaces importieren, bevor Sie die Business Space-Umgebung verwenden können. Führen Sie die Schritte aus, die im Abschnitt Aktualisierung von Business Space-Vorlagen und Spaces nach der Installation oder Aktualisierung von Widgets beschrieben sind.
- Aktualisieren Sie die Endpunkte für die Widgets, die in Business Space bereitgestellt werden sollen.
  - Richten Sie die Sicherheitsfunktion für Business Space und die von Ihrem Team verwendeten Widgets ein.

### **REST-Serviceendpunkte von Business Space-Widgets über die Befehlszeile registrieren:**

Wenn Sie Business Space über die Administrationskonsole konfigurieren, müssen Sie die REST-Endpunkte so registrieren, dass Ihr Team die Widgets in Business Space verwenden kann. Wenn Sie die Endpunkte nicht über die Seiten 'Business Space - Konfiguration' und 'REST-Serviceendpunkt - Registrierung' der Administrationskonsole registrieren, können Sie den Befehl **registerRESTServiceEndpoint** verwenden.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Installieren Sie das Produkt.
- Konfigurieren Sie die REST-Services für die Widgets, die Sie in Business Space verwenden, über die Seite der Administrationskonsole für REST-Services oder mit dem Befehl **updateRESTGatewayService**. Wenn Sie eine eigenständige Serverumgebung haben oder die Laufzeitumgebung mit dem Assistenten für die Implementierungsumgebung konfigurieren, werden die REST-Services automatisch konfiguriert und aktiviert.

- Konfigurieren Sie Business Space auf der Seite 'Business Space - Konfiguration' der Administrationskonsole oder mit den Befehlen **installBusinessSpace** und **configureBusinessSpace**.
- Konfigurieren Sie die Datenbanktabellen (bei Verwendung einer fernen Datenbank oder einer Network Deployment-Umgebung).

REST-Services werden automatisch registriert, wenn Sie eine eigenständige Serverumgebung haben und Sie Business Space mit der Administrationskonsole oder dem Profile Management Tool konfiguriert haben, oder wenn Sie Ihre Laufzeitumgebung mit dem Assistenten für die Implementierungsumgebung konfiguriert haben. Andernfalls müssen Sie die REST-Services konfigurieren und anschließend registrieren.

Sie können die Seite 'REST-Serviceendpunkt - Registrierung' der Administrationskonsole oder den Befehl **registerRESTServiceEndpoint** verwenden, um die REST-Serviceendpunkte für alle Widgets Ihres Produkts in Business Space zu registrieren. Anschließend ordnet Business Space diesen Endpunkten automatisch Widgets zu und die Widgets werden zur Verwendung in der Palette von Business Space angezeigt.

Sie können den Befehl **registerRESTServiceEndpoint** verwenden, um eine Gruppe von Endpunkten für einen bestimmten Provider, ein Implementierungsziel oder alle eindeutigen Endpunkte in einer Zelle zu registrieren. Dieser Befehl registriert die Endpunkte der REST-Services, die sich in derselben Zelle wie Business Space befinden.

1. Öffnen Sie ein Befehlsfenster.

Der Befehl 'wsadmin' befindet sich in einer eigenständigen Serverumgebung im Verzeichnis *stammverzeichnis\_des\_profils/bin* und in einer Network Deployment-Umgebung im Verzeichnis *stammverzeichnis\_des\_deployment\_manager\_profils/bin*.

2. Geben Sie an der Eingabeaufforderung **wsadmin** ein, um die **wsadmin**-Umgebung zu starten.
3. Mit dem Befehl **registerRESTServiceEndpoint** können Sie die Business Space-Endpunkte für die REST-Services aller Widgets Ihres Produkts registrieren.
4. Führen Sie nach jedem Befehl den Befehl 'save' aus.

Im folgenden Beispiel wird mit Jython der Befehl **registerRESTServiceEndpoint** ausgeführt. Anschließend werden die Änderungen gespeichert. Alle konfigurierten und aktivierten REST-Services in dem Cluster werden bei Business Space registriert.

```
AdminTask.registerRESTServiceEndpoint('[-clusterName
  name_des_rest-services-cluster -businessSpaceClusterName
  name_des_business_space-clusters]')
AdminConfig.save()
```

Dabei ist *name\_des\_rest\_service\_clusters* der Name des Clusters, in dem die REST-Services konfiguriert werden, und *name\_des\_business\_space\_clusters* der Name des Clusters, in dem Business Space implementiert wird.

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask registerRESTServiceEndpoint
{-clusterName name_des_rest_service_clusters
-businessSpaceClusterName name_des_business_space_clusters}
$AdminConfig save
```

Dabei ist *name\_des\_rest\_service\_clusters* der Name des Clusters, in dem die REST-Services konfiguriert werden, und *name\_des\_business\_space\_clusters* der Name des Clusters, in dem Business Space implementiert wird.

Die Parameter **appName**, **webModuleName**, **type**, **name**, **version**, **nodeName**, **serverName** und **clusterName** sind optional.

Wenn Sie die Parameter **type**, **appName** und **webModuleName** nicht angeben, werden alle auf dem Implementierungsziel konfigurierten, eindeutigen REST-Serviceendpunkte registriert.

Wenn Sie keinen dieser Parameter angeben, werden alle auf einem beliebigen Implementierungsziel konfigurierten, eindeutigen REST-Serviceendpunkte registriert.

**Tipp:** Business Space verwendet eine Proxy-Serverkomponente, um eine Verbindung zu Ihren REST-Services herzustellen. Falls die REST-Services nicht immer reagieren, müssen Sie die Einstellungen für das Verbindungszeitlimit zwischen Business Space und Ihren REST-Services aktualisieren, je nachdem, wie die Leistung auf den Servern für die REST-Services ist. Weitere Informationen enthält der Abschnitt Einstellung für die Zeitlimitüberschreitung für den Business Space-Ajax-Proxy ändern.

#### **Virtuellen Host vom primären Cluster-Member entfernen:**

In manchen Network Deployment-Topologien muss der Administrator unter Umständen den virtuellen Host manuell aus dem primären Cluster-Member entfernen, damit der gesamte Datenverkehr über einen Web-Server abgewickelt wird. Die Konfiguration eines Business Space in einem Cluster stellt den virtuellen Host wieder her, eventuell sollte der virtuelle Host gelöscht werden, damit Ihre Umgebung so arbeitet, wie sie ursprünglich eingerichtet wurde.

Business Space benötigt einen Cluster-Member zum Ausführen von Ladeoperationen beim ersten Systemstart des Servers. Wenn der primäre Cluster-Member über keinen virtuellen Host verfügt, dann fügt die Business Space-Konfiguration einen virtuellen Host hinzu, der die ersten Ladeoperationen ausführt.

Prüfen Sie nach der Konfiguration des Business Space in einem Cluster die Liste WebSphere Application Server *default\_host* darauf, ob sie einen virtuellen Host für den primären Cluster-Member enthält.

Damit auf den virtuellen Host nicht mehr zugegriffen werden kann, führen Sie eine der folgenden Aktionen aus.

- Inaktivieren Sie den virtuellen Host für den primären Cluster-Member nach dem ersten Start des Clusters.
- Löschen Sie den virtuellen Host für den primären Cluster-Member über die Administrationskonsole (klicken Sie auf **Umgebung** > **Virtuelle Hosts** > *default\_host* > **Hostaliasnamen**) oder benutzen Sie die entsprechenden Befehle (siehe Arbeiten mit Eigenschaftsdateien für virtuelle Hosts in der Dokumentation für WebSphere Application Server).

#### **Proxy-Server oder Lastausgleichsserver für Verwendung mit Business Space konfigurieren:**

Wenn Sie Business Space in einer Umgebung mit einem Proxy-Server oder einem Lastausgleichsserver verwenden, müssen Sie Ihre Umgebung so einrichten, dass Business Space und die Widgets ordnungsgemäß funktionieren können.

In einer Network Deployment- oder Clusterumgebung richten Sie möglicherweise einen Proxy-Server oder einen HTTP-Server aus Sicherheitsgründen sowie zu Routing- und Lastausgleichszwecken ein. Eingehende HTTP-Anforderungen gehen dadurch nicht direkt an einen Anwendungsserver, sondern an einen Proxy-Server, der die Anforderungen über mehrere Anwendungsserver verteilt, die die Verarbeitungen ausführen.

Sie können weitere Routing-Server anstelle oder vor dem Proxy-Server verwenden, z. B. IBM HTTP Server.

**Wichtig:** Der Proxy-Server (oder ein alternativer Routing-Server) ist für HTTP-Anforderungen für den Lastausgleich zwischen zwei oder mehreren Cluster-Members erforderlich. Der Proxy-Server ermöglicht es den Clients, auf die Anwendungen in dieser Topologie zuzugreifen.

Stellen Sie in einer Umgebung mit einem Lastausgleichsserver oder einem Proxy-Server zwischen dem Browser sowie Business Space und den REST-Services sicher, dass das, was Sie für das REST-Serviceprotokoll, den Host und den Port festlegen, der Browser-URL für den Zugriff auf Business Space entspricht. Prüfen Sie auf der Seite für den REST-Service-Provider in der Administrationskonsole, ob für alle Provider wie z. B. den Business Flow Manager und den Human Task Manager das Protokoll sowie Host und Port korrekt festgelegt sind. Weitere Informationen zum Ändern von REST-Services finden Sie im Abschnitt REST-Services in einem Service-Provider konfigurieren.

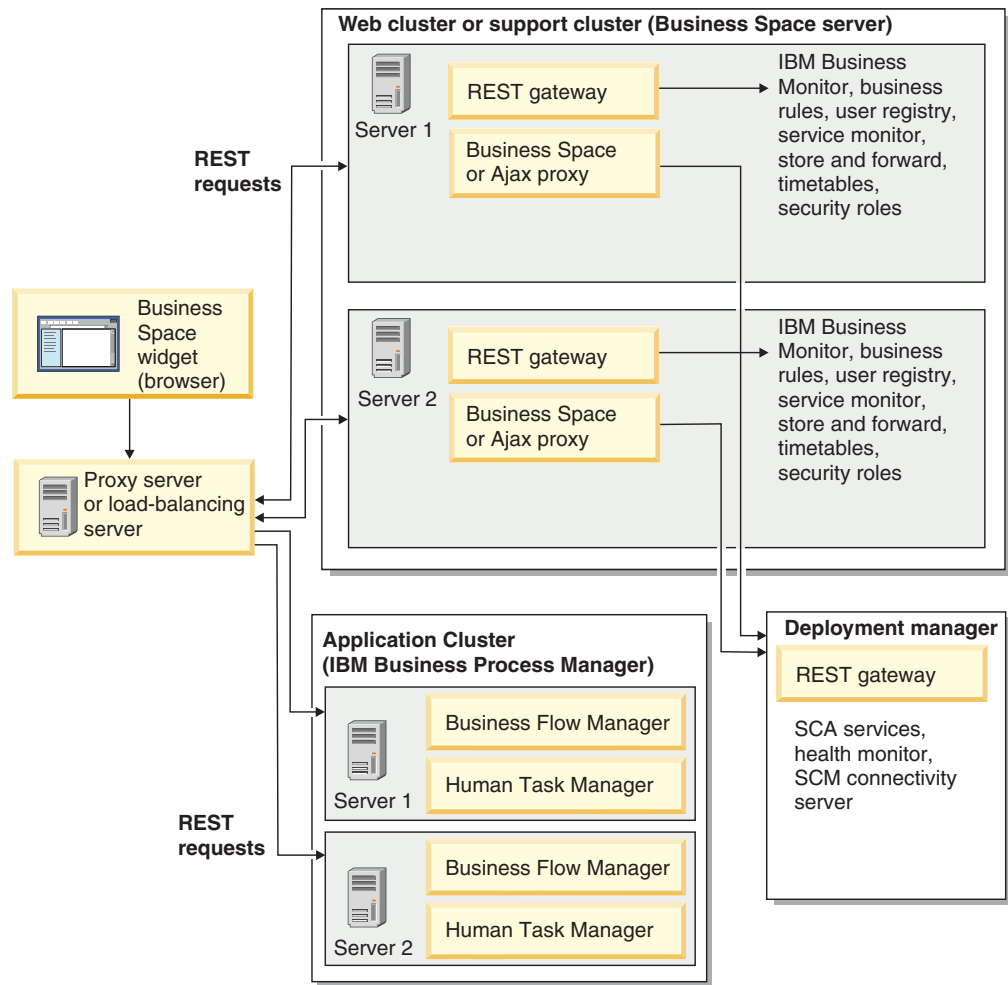


Abbildung 1. Typische Topologie

Wenn Sie IBM HTTP Server verwenden, müssen Sie zusätzliche Zuordnungsschritte ausführen, um sicherzustellen, dass die Module dem Web-Server zugeordnet sind und dass die Hostalies konfiguriert sind.

Bei Verwendung eines WebSphere Application Server-Proxy-Servers müssen Sie sicherstellen, dass alle Module für den Proxy-Server aktiviert wurden.

Wenn Sie eine Reverse Proxy-Konfiguration für einen HTTP-Server verwenden, müssen Sie die URLs für Business Space und die Widgets zuordnen.

*IBM HTTP Server für Business Space konfigurieren:*

Wenn Sie IBM HTTP Server verwenden, müssen Sie zusätzliche Zuordnungsschritte ausführen, um sicherzustellen, dass Business Space in Ihrer Umgebung funktioniert.

Führen Sie zunächst folgende Schritte vor der Konfiguration von IBM HTTP Server für die Arbeit mit Business Space aus:

- Installieren Sie IBM HTTP Server.
- Stellen Sie sicher, dass Secure Sockets Layer (SSL) für IBM HTTP Server aktiviert ist.

- Stellen Sie sicher, dass die Web-Server-Definition für IBM HTTP Server dem Anwendungsserver hinzugefügt wurde.

Während der Installation des IBM HTTP Server-Plug-ins wird von dem Installationsprozess auf dem Web-Serversystem das Script `configureWeb_server` produziert. Das Script `configureWeb_server` ist dazu gedacht, Webanwendungsmodulen dem Web-Server zuzuordnen. Führen Sie daher dieses Script nach der Generierung der Implementierungsumgebung aus.

1. Stellen Sie sicher, dass dem Web-Server die Module zugeordnet wurden. Prüfen Sie für alle Anwendungen, die für Business Space erforderlich sind, ob der Web-Server eins der ausgewählten Ziele ist.
  - a. Melden Sie sich an der Administrationskonsole als Benutzer mit Verwaltungsaufgaben an.
  - b. Klicken Sie auf **Anwendungen > Anwendungstypen > WebSphere Enterprise-Anwendungen**.
  - c. Klicken Sie über die Enterprise-Anwendungsanzeige auf den Namen der Anwendung.

Überprüfen Sie die folgenden Anwendungen. Sie verfügen möglicherweise über alle oder nur einige der Anwendungen in der Liste, je nachdem, welche Produkte Sie mit Business Space verwenden.

- Für alle Produkte:
  - `BSpaceEAR_knotenname_servername`
  - `BSpaceForms_knotenname_servername`
  - `BSpaceHelp_knotenname_servername`
  - `BusinessSpaceHelpEAR_knotenname_servername`
  - `REST-Services-Gateway`
  - `mm.was_knotenname_servername`
  - `PageBuilder2_knotenname_servername`
- Für IBM Business Process Manager:
  - `BPCExplorer_knotenname_servername` (nur für IBM BPM Advanced)
  - `BPEContainer_knotenname_servername` (nur für IBM BPM Advanced)
  - `BPMAdministrationWidgets_knotenname_servername` (nur für IBM BPM Advanced)
  - `HumanTaskManagementWidgets_knotenname_servername` (nur für IBM BPM Advanced)
  - `IBM_BPM_Help_knotenname_servername`
  - `IBM_BPM_PerformanceDW_knotenname_servername`
  - `IBM_BPM_Portal_knotenname_servername`
  - `IBM_BPM_ProcessAdmin_knotenname_servername`
  - `IBM_BPM_Process_Portal_Notification_knotenname_servername`
  - `IBM_BPM_Process_Portal_knotenname_servername`
  - `IBM_BPM_Repository_knotenname_servername` (nur für Process Center)
  - `IBM_BPM_Teamworks_knotenname_servername`
  - `IBM_BPM_WebAPI_knotenname_servername`
  - `REST Services Gateway Dmgr` (nur für IBM BPM Advanced)
  - `TaskContainer_knotenname_servername`
- Für WebSphere Enterprise Service Bus:
  - `BPMAdministrationWidgets_knotenname_servername`



- REST Services Gateway Dmgr
  - `wesbWidgets_knotenname_servername`
  - Für IBM Business Monitor:
    - `HumanTaskManagementWidgets_knotenname_servername`
    - `WBMDashboardWeb_knotenname_servername`
- d. Klicken Sie für all diese Anwendungen in der Konfigurationsregisterkarte unter 'Module' auf **Module verwalten**.
  - e. Stellen Sie auf der Seite **Module verwalten** für Ihre Anwendung sicher, dass der Web-Server einer der ausgewählten Ziele all Ihrer Module ist.
    - Prüfen Sie für die einzelnen Module in der Tabelle die Spalte "Server", um sicherzustellen, dass der Web-Server einer der ausgewählten Ziele all Ihrer Module ist. Beispiel: Suchen Sie für die Anwendung `mm.was_knotenname_servername` nach dem Web-Server, der in der Spalte 'Server' angezeigt werden soll:  
**WebSphere:cell=qaxs41Cell02,node=qaxs41Node03,server=httpserver**  
**WebSphere:cell=qaxs41Cell02,cluster=Golden.WebApp.**
    - Falls der Web-Server hinzugefügt werden muss, wählen Sie das Kontrollkästchen neben dem Namen des betreffenden Moduls. Verwenden Sie dann in der Liste mit den Clustern und Servern die Steuertaste, um mehrere Ziele auszuwählen. Beispiel: Wenn Sie für Ihre Anwendung einen Web-Server bereitstellen möchten, drücken Sie die Steuertaste und wählen Sie anschließend den Cluster von Anwendungsservern und den Web-Server gleichzeitig aus. Klicken Sie auf **Anwenden**, **OK** und **Speichern**, um etwaige Änderungen zu speichern.
2. Prüfen Sie, ob der Alias des Hostnamens `default_host` für alle Cluster-Member, Web-Server oder Proxy-Server die korrekten Informationen enthält.
    - a. Melden Sie sich an der Administrationskonsole als Benutzer mit Verwaltungsaufgaben an.
    - b. Klicken Sie auf **Server > Servertypen > WebSphere-Anwendungsserver**.
    - c. Klicken Sie für jedes Cluster-Member auf den Anwendungsservernamen, um die Portnummer für den Portnamen `WC_defaulthost` anzuzeigen.
      - Erweitern Sie unter 'Übertragungen' die Option **Ports**.
      - Notieren Sie sich für den Portnamen `WC_defaulthost` dessen Portnummer.
    - d. Klicken Sie über den linken Navigationsbereich der Administrationskonsole auf **Umgebung > Virtuelle Hosts**.
    - e. Klicken Sie auf den Namen `default_host`.
    - f. Klicken Sie unter 'Weitere Eigenschaften' auf **Hostaliasnamen**.
    - g. Werden Hostname und Portnummer für die Cluster-Member nicht in der Liste angezeigt, klicken Sie auf **Neu**, um den fehlenden Eintrag in die Liste aufzunehmen. Für den Hostnamen wird das Platzhalterzeichen \* (Stern) unterstützt.
    - h. Wenn Sie einen neuen Eintrag hinzufügen, klicken Sie auf **Speichern** und **Synchronisieren**.
  3. Beim kombinierten Einsatz eines HTTP-Server-Vorrechners mit Business Space müssen Sie für das Web-Server-Plug-in in der Administrationskonsole von WebSphere Application Server unter **Web-Server > webserver1 > Plug-in-Eigenschaften > Anforderung und Antwort** die Anforderung **Accept content for all requests** (Inhalt für alle Anforderungen übernehmen) auf `true` (wahr) setzen.

*WebSphere Application Server-Proxy-Server für Business Space konfigurieren:*

Bei Verwendung eines WebSphere Application Server-Proxy-Servers müssen Sie sicherstellen, dass alle Module für den Proxy-Server aktiviert wurden, damit Business Space in Ihrer Umgebung ausgeführt werden kann.

Führen Sie zunächst folgende Schritte vor der Konfiguration des WebSphere Application Server-Proxy-Servers für die Arbeit mit Business Space aus:

1. Stellen Sie sicher, dass Sie die aktuelle Version von WebSphere Application Server angewendet haben.
2. Erstellen Sie einen Proxy-Server. Klicken Sie dazu auf **Server > Servertypen > WebSphere-Proxy-Server**. Weitere Informationen zu diesem Thema finden Sie im Abschnitt Proxy-Server einrichten im Information Center von WebSphere Application Server.
3. Stellen Sie sicher, dass das HTTP-Protokoll ausgewählt ist.
1. Optional: Stellen Sie sicher, dass dem WebSphere Application Server-Proxy-Server Module zugeordnet wurden. Prüfen Sie für alle Anwendungen, die für Business Space erforderlich sind, dass die Module für den Proxy-Server aktiviert wurden.
  - a. Melden Sie sich bei der Administrationskonsole als Benutzer mit Verwaltungsaufgaben an.
  - b. Wählen Sie **Anwendungen > Anwendungstypen > WebSphere Enterprise-Anwendungen** aus.
  - c. Wählen Sie über die Anzeige 'Enterprise-Anwendungen' den Namen der Anwendung aus.

Überprüfen Sie die folgenden Anwendungen. Sie verfügen möglicherweise über alle oder nur einige der Anwendungen in der Liste, je nachdem, welche Produkte Sie mit Business Space verwenden.

- Für alle Produkte:
  - **BSpaceEAR\_knotenname\_servername**
  - **BSpaceForms\_knotenname\_servername**
  - **BSpaceHelp\_knotenname\_servername**
  - **BusinessSpaceHelpEAR\_knotenname\_servername**
  - **REST-Services-Gateway**
  - **mm.was\_knotenname\_servername**
  - **PageBuilder2\_knotenname\_servername**
- Für IBM Business Process Manager:
  - **BPCExplorer\_knotenname\_servername** (nur für IBM BPM Advanced)
  - **BPEContainer\_knotenname\_servername** (nur für IBM BPM Advanced)
  - **BPMAdministrationWidgets\_knotenname\_servername** (nur für IBM BPM Advanced)
  - **HumanTaskManagementWidgets\_knotenname\_servername** (nur für IBM BPM Advanced)
  - **IBM\_BPM\_Help\_knotenname\_servername**
  - **IBM\_BPM\_PerformanceDW\_knotenname\_servername**
  - **IBM\_BPM\_Portal\_knotenname\_servername**
  - **IBM\_BPM\_ProcessAdmin\_knotenname\_servername**
  - **IBM\_BPM\_Process\_Portal\_Notification\_knotenname\_servername**
  - **IBM\_BPM\_Process\_Portal\_knotenname\_servername**
  - **IBM\_BPM\_Repository\_knotenname\_servername** (nur für Process Center)

- *IBM\_BPM\_Teamworks\_knotenname\_servername*
  - *IBM\_BPM\_WebAPI\_knotenname\_servername*
  - **REST Services Gateway Dmgr** (nur für IBM BPM Advanced)
  - *TaskContainer\_knotenname\_servername*
  - Für WebSphere Enterprise Service Bus:
    - *BPMAdministrationWidgets\_knotenname\_servername*
    - **REST Services Gateway Dmgr**
    - *wesbWidgets\_knotenname\_servername*
  - Für IBM Business Monitor:
    - *HumanTaskManagementWidgets\_knotenname\_servername*
    - *WBMDashboardWeb\_knotenname\_servername*
- d. Prüfen Sie für jede Anwendung, ob sie den Wert `default_host` verwendet, indem Sie auf den Namen der Anwendung und anschließend auf **Virtuelle Hosts** klicken.
  - e. Klicken Sie für jede Anwendung auf der Registerkarte **Konfiguration** unter **Module** auf **Module verwalten** und anschließend auf der Seite **Module verwalten** für die Anwendung auf jedes Modul und wählen Sie **Proxy-Konfiguration des Webmoduls** aus. Prüfen Sie, ob **Proxy aktivieren** ausgewählt ist.
2. Prüfen Sie, ob der Alias des Hostnamens `default_host` für alle Cluster-Member, Web-Server oder Proxy-Server die korrekten Informationen enthält.
    - a. Melden Sie sich bei der Administrationskonsole als Benutzer mit Verwaltungsaufgaben an.
    - b. Wählen Sie **Server > Servertypen > WebSphere-Anwendungsserver** aus.
    - c. Wählen Sie für jedes Cluster-Member den Anwendungsservernamen aus, um die Portnummer für den Portnamen **WC\_defaulthost** anzuzeigen.
      - Erweitern Sie unter 'Übertragungen' die Option **Ports**.
      - Notieren Sie sich die Portnummer des Ports **WC\_defaulthost**.
    - d. Wählen Sie im linken Navigationsbereich der Administrationskonsole **Umgebung > Virtuelle Hosts** aus.
    - e. Klicken Sie auf **default\_host**.
    - f. Klicken Sie unter 'Weitere Eigenschaften' auf **Hostaliasnamen**.
    - g. Werden Hostname und Portnummer für die Cluster-Member nicht in der Liste angezeigt, klicken Sie auf **Neu**, um den fehlenden Eintrag in die Liste aufzunehmen. Für den Hostnamen können Sie das Platzhalterzeichen \* (Stern) verwenden.
    - h. Wenn Sie einen neuen Eintrag hinzufügen, klicken Sie auf **Speichern** und dann auf **Synchronisieren**.
  3. Zur Verwendung des HTTP-Protokolls müssen Sie den WebSphere Application Server-Proxy-Server konfigurieren.
    - a. Melden Sie sich bei der Administrationskonsole als Benutzer mit Verwaltungsaufgaben an.
    - b. Wählen Sie **Server > Servertypen > WebSphere-Proxy-Server** aus und wählen Sie dann den zuvor erstellten Proxy-Server aus.
    - c. Erweitern Sie **HTTP-Einstellungen für Proxy-Server** und klicken Sie auf **Proxy-Einstellungen**.
    - d. Klicken Sie auf **Angepasste Eigenschaften** und fügen Sie die neue Eigenschaft `cache.query.string` mit dem Wert `true` hinzu.

- e. Klicken Sie auf **Speichern** und führen Sie einen Neustart des Proxy-Servers durch.

*Business Space-URLs für einen Reverse Proxy-Server zuordnen:*

Wenn Ihr HTTP-Server über eine Reverse Proxy-Konfiguration verfügt und dieser Server für Business Space konfiguriert wird, müssen Sie die URLs Business Space und den von Ihrem Team verwendeten Widgets zuordnen.

1. Bearbeiten Sie die Konfigurationsdatei des HTTP-Servers.
2. Ordnen Sie alle URLs Business Space und den Widgets zu, mit denen die Geschäftsbenutzer in der Laufzeitlösung arbeiten.

URLs für allgemeines Business Space-Framework (alle Produkte):

- /BusinessSpace/\*
- /mum/\*
- /BusinessSpaceHelp/\*
- /BspaceWebformsProxy/\*
- /themes/\*
- /pageBuilder2/\*

Zusätzliche URLs für IBM Business Monitor-Widgets:

- /BusinessDashboard/\*
- /DashboardABX/\*
- /monitorServerComponent/\*
- /mobile/\*
- /rest/\*
- /p2pd/\*
- /AlphabloxServer/\*
- /AlphabloxAdmin/\*
- /AlphabloxTooling/\*
- /BloxBuilder/\*

Zusätzliche URLs für IBM Business Process Manager Advanced-Widgets:

- /BspaceWidgetsHM/\*
- /SecurityManagerWidgets/\*
- /BspaceWidgetsBCM/\*
- /rest/\*
- /ProcessPortal/\*
- /PolymorphicWidget/\*
- /scaWidget/\*
- /ServiceMonitorGraphWidget/\*
- /StoreAndForward/\*

Zusätzliche URL für IBM Business Process Manager Standard zur Arbeit mit Process Portal:

- /ProcessPortal/\*

Zusätzliche URLs für WebSphere Enterprise Service Bus-Widgets:

- /BspaceWidgetsHM/\*
- /rest/\*
- /PolymorphicWidget/\*
- /scaWidget/\*

- /ServiceMonitorGraphWidget/\*
- /StoreAndForward/\*

### Federation API über mehrere Implementierungsziele hinweg aktivieren:

Die Federation API gibt Ihnen die Möglichkeit, Prozesse und Tasks anzuzeigen, die in Process Designer und Integration Designer in derselben Taskliste erstellt wurden. Wenn Ihre Umgebung mehrere Cluster in derselben Zelle enthält oder wenn sie mehrere Zellen umfasst, müssen Sie die Föderationsdomänen mit Befehlen manuell konfigurieren.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Process Manager Advanced
- IBM Business Process Manager Standard

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Installieren Sie das Produkt.
- Erstellen Sie Profile und konfigurieren Sie Business Space auf einem Implementierungsziel (Server oder Cluster).
- Konfigurieren Sie die Datenbanktabellen (bei Verwendung einer fernen Datenbank oder einer Implementierungsumgebung).

Die Federation API wird automatisch mit Ihrem Produkt als Teil der REST Services Gateway-Anwendung konfiguriert. Wenn Sie diese Konfiguration für Ihre Umgebung mit mehreren Implementierungszielen ändern wollen, verwenden Sie `wsadmin`-Befehle.

1. Öffnen Sie ein Befehlsfenster.

Der Befehl `'wsadmin'` befindet sich in einer eigenständigen Serverumgebung im Verzeichnis `stammverzeichnis_des_profils/bin` und in einer Network Deployment-Umgebung im Verzeichnis `stammverzeichnis_des_deployment_manager_profils/bin`.

2. Geben Sie bei der Eingabeaufforderung `wsadmin` ein, um die `wsadmin`-Umgebung zu starten.
3. Verwenden Sie den Befehl `createBPMapiFederationDomain` mit dem Schritt `addTarget`, um eine Föderationsdomäne zu erstellen, die sich über ein oder mehrere Implementierungsziele erstreckt.

Für den Namensparameter muss ein eindeutiger *name\_für\_die\_föderationsdomäne* angegeben werden.

Das folgende Beispiel fügt eine Föderationsdomäne mit dem Namen `myCustomFederationDomain` hinzu, die sich über einen Server (mit dem Knotennamen `myNode` und dem Servernamen `myServer`) und einen Cluster (mit dem Namen `myCluster`) erstreckt.

- Beispiel mit Jython:

```
AdminTask.createBPMapiFederationDomain(['-nodeName knotenname
-serverName servername -name myCustomFederationDomain -addTarget [{"
myNode myServer ""} [{" "" "" "" myCluster}]]')
```

- Beispiel mit Jacl:

```
$AdminTask createBPMapiFederationDomain {-nodeName knotenname
-serverName servername -name myCustomFederationDomain -addTarget {{""
myNode myServer ""} {" "" "" "" myCluster}}}
```

Weitere Befehle stehen zur Verfügung für den Fall, dass Sie die Federation API-Konfiguration ändern müssen.

- Wenn Sie eine Föderationsdomäne einschließlich der enthaltenen Ziele löschen wollen, verwenden Sie den Befehl **deleteBPMApiFederationDomain**.
- Um alle Föderationsdomänen aufzulisten, verwenden Sie den Befehl **listBPMApiFederationDomains**.
- Wenn Sie Ziele zu einer Föderationsdomäne hinzufügen oder aus ihr entfernen wollen, verwenden Sie den Befehl **modifyBPMApiFederationDomain**.
- Wenn Sie Details über eine Föderationsdomäne anzeigen möchten, verwenden Sie den Befehl **showBPMApiFederationDomain**.

### **Business Space-Widgets für zellenübergreifende Umgebungen aktivieren:**

Sie müssen die Endpunktdateien manuell bearbeiten, wenn Business Space in einer anderen Zelle als die REST-Services ausgeführt wird, oder wenn die Widgets in anderen Zellen als Business Space sind.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Installieren Sie das Produkt.
- Erstellen Sie Profile und konfigurieren Sie Business Space auf einem Implementierungsziel (Server oder Cluster).
- Konfigurieren Sie die Datenbanktabellen (bei Verwendung einer fernen Datenbank oder einer Implementierungsumgebung).

Alle für Ihr Produkt benötigten Widgets werden zusammen mit Business Space installiert, die von den Widgets benötigten Endpunkte müssen jedoch konfiguriert und registriert werden, bevor Ihr Team die Widgets in Business Space verwenden kann. Sie können die Endpunkte über die Seiten der Administrationskonsole konfigurieren und registrieren. Wenn Ihr Produkt und die REST-Services jedoch in einer anderen Zelle als Business Space installiert sind, müssen Sie die REST-Serviceendpunktdateien so bearbeiten, dass sie in Business Space auf die REST-Services zugreifen und Ihre Widgets ordnungsgemäß funktionieren.

Bearbeiten Sie je nach den installierten Produkten eine oder mehrere der Serviceendpunktdateien und Widgetendpunktdateien sowie die in Business Space verwendeten Widgets. Üblicherweise enthalten Serviceendpunktdateien den Namensbestandteil `Endpoint` oder `Endpoints` im XML-Dateinamen und Widgetendpunktdateien analog dazu den Namensbestandteil `Widget` oder `Widgets` im XML-Dateinamen. Die folgende Liste enthält IBM Geschäftsprozessmanagementbeispiele von Serviceendpunktdateien und Widgetendpunktdateien:

- IBM Business Monitor: `monitorEndpoints.xml` und `monitorWidget.xml`
- IBM Business Monitor mit IBM Cognos Business Intelligence: `cognosEndpoints.xml` und `cognosWidget.xml`
- WebSphere Enterprise Service Bus: `wesbWidgetEndpoints.xml` (für Widgets 'Mediationsrichtlinienverwaltung', 'Service-Browser' und 'Proxy-Gateway'), `bpmAdministrationEndpoints.xml` und `BPMAdministrationWidgetEndpoints.xml` (für Widgets 'Verwaltung')
- IBM Business Process Manager: `wpsEndpoints.xml`, `bpmAdministrationEndpoints.xml` und `BPMAdministrationWidgetEndpoints.xml` (für Widgets 'Verwaltung'), `wesbWidgetEndpoints.xml` (für Widgets 'Mediationsrichtlinienverwaltung', 'Service-Browser' und 'Proxy-Gateway'),



HumanTaskManagementEndpoints.xml für Business-Prozesse und Benutzertasks, bspaceWFSEndpoints.xml (für die Verwendung von Lotus Webform Server mit den Widgets 'Benutzertaskverwaltung').

- Alle Produkte: wsumEndpoint.xml und wsumWidget.xml (für Benutzerzugehörigkeit)

Wenn Sie über Administratorberechtigungen verfügen, dann können Sie Endpunkte registrieren und Widgets aktivieren, indem Sie die folgenden Arbeitsschritte ausführen.

1. Kopieren Sie die im ZIP-Verzeichnis *installationsstammverzeichnis\BusinessSpace\registryData\produktname\produktname\_widget\_vergebener\_name\_crosscell.zip* befindliche ferne, komprimierte Widget-Datei in die Zelle, in der Business Space während der Produktinstallation konfiguriert wird. Die Widgets befinden sich in diesem Verzeichnis und können in einen temporären Ordner kopiert werden.
2. Entpacken Sie das *crosscell.zip* in einen temporären Ordner.
3. Suchen Sie die Serviceendpunkt- und Widgetendpunktdateien.  
Wechseln Sie von dem Verzeichnis, in das Sie die ZIP-Datei entpackt haben, in das Unterverzeichnis *endpoints*, um alle Widgetendpunktdateien und Serviceendpunktdateien anzuzeigen. Typischerweise enden die Dateinamen alle mit *Endpoints.xml* oder *Endpoint.xml*.

4. Konfigurieren Sie die Endpunkte nach Bedarf durch Bearbeitung der Serviceendpunktdateien und Widgetendpunktdateien.

- a. Bearbeiten Sie die Serviceendpunktdateien so, dass sie auf den Service verweisen.

Jeder Endpunkt in der Serviceendpunktdatei wird durch einen Block `<tns:Endpoint>` definiert. Identifizieren Sie den zu ändernden Block. Suchen Sie nach Kommentaren, die Ihnen einen Hinweis darauf geben, wo Sie die Bearbeitung vornehmen müssen, zum Beispiel:

```
<!-- Befindet sich der REST-Service nicht lokal auf Ihrem Business Space-Server, aktualisiere  
<tns:url>/rest/bpm/monitor/</tns:url>
```

**Tipp:** Wenn Sie vorhaben, bestimmte Endpunkte nicht zu aktivieren, können Sie diese aus der Datei entfernen, um Unklarheiten zu vermeiden.

Die durch einen Endpunkt identifizierte Position wird in `<tns:url>` angegeben. Dieser Wert ist ein Pfad in einem Webmodul, der als vollständige oder relative HTTP-URL angegeben wird. Standardmäßig wird eine relative URL angegeben. Ändern Sie diese Angabe in einen vollständigen URL-Pfad, z. B. `https://virtueller_host.com:virtueller_port/rest/bpm/htm` oder `http://host1:9445/WBPublishingDRAFT/`. Das Protokoll, der Host und der Port geben an, wie der Zugriff auf das Webmodul des Produkts erfolgt.

Führen Sie die folgenden Arbeitsschritte aus, um die Portnummer für den Server zu suchen:

- Melden Sie sich an der Administrationskonsole an.
- Klicken Sie auf **Server > Servertypen > WebSphere-Anwendungsserver**.
- Klicken Sie auf den Server, dessen Portnummer gesucht werden soll, und erweitern Sie dann die Anzeige des Abschnitts für die Ports.

Alle Anwendungen verwenden denselben Port, der im Parameter **wc\_defaulthost** (nicht gesicherter Host) oder im Parameter **wc\_defaulthost\_secure** (gesicherter Host) angegeben ist.

**Tipp:** Wenn Sie einen HTTP-Server verwenden, um auf Ihre Webmodule für den Lastausgleich zuzugreifen, verwenden Sie den Hostnamen und die Porteneinstellungen des HTTP-Servers.

- b. Bearbeiten Sie die Widgetendpunktdateien so, dass sie auf die Speicherposition von Business Space verweisen, auf der die Widgets implementiert sind.

Jeder Endpunkt in der Serviceendpunktdatei wird durch einen Block `<tns:id>` definiert. Identifizieren Sie den zu ändernden Block. Suchen Sie nach Kommentaren, die Ihnen einen Hinweis darauf geben, wo Sie die Bearbeitung vornehmen müssen, zum Beispiel:

```
<!-- Werden Widgets in einer über Fernzugriff angebotenen Konfiguration verwendet, aktualisiere -->
<tns:url>/BusinessDashboard/</tns:url>
```

Die durch einen Endpunkt identifizierte Position wird in `<tns:url>` angegeben. Ändern Sie diese Angabe in einen vollständigen URL-Pfad, der auf die Speicherposition von Business Space verweist, auf der die Widgets implementiert sind; Beispiel:`https://host.domain.com:port/BusinessDashboard/`

5. Führen Sie in der Zelle, in der der Business Space-Server konfiguriert ist, den Befehl **updateBusinessSpaceWidgets** aus, um die Endpunkt-URL-Dateien zu aktualisieren, nachdem Sie die Endpunkt-XML-Dateien modifiziert haben.
  - a. Öffnen Sie für Ihr Profil ein Befehlsfenster. Der Befehl 'wsadmin' befindet sich im Verzeichnis `profiles\profilname\bin`. Führen Sie den Befehl in einer Clusterumgebung im Verzeichnis `stammverzeichnis_des_deployment_manager-profil\bin` aus. Führen Sie den Befehl in einer eigenständigen Serverumgebung im Verzeichnis `stammverzeichnis_des_profil\bin` aus.
  - b. Geben Sie an der Eingabeaufforderung **wsadmin** ein, um die **wsadmin**-Umgebung zu starten.
  - c. Führen Sie den Befehl **updateBusinessSpaceWidgets** aus. Geben Sie in einer Clusterumgebung den Parameter **-clusterName** an. Geben Sie in einer eigenständigen Serverumgebung die Parameter **-serverName** und **-nodeName** an. Geben Sie den Parameter **-endpoints** mit dem vollständigen Pfad zu dem Verzeichnis, in das Sie die Widgetendpunktdateien entpackt haben. Geben Sie den Parameter **-catalogs** an, um auf das Verzeichnis zu verweisen, in das Sie die Widgetendpunktdateien entpackt haben.
6. Starten Sie den Server erneut.

Die folgende Endpunktbeispieldatei gilt für IBM Business Monitor-Widgets.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- START NON-TRANSLATABLE -->
<tns:BusinessSpaceRegistry
  xmlns:tns="http://com.ibm.bspace/BusinessSpaceRegistry"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://com.ibm.bspace/BusinessSpaceRegistry
  BusinessSpaceRegistry.xsd ">

  <tns:Endpoint>
    <tns:id>{com.ibm.wbimonitor}monitorServiceRootId</tns:id>
    <tns:type>{com.ibm.wbimonitor}monitorServiceRootId</tns:type>
    <tns:version>1.0.0.0</tns:version>
    <tns:url>/rest/</tns:url>
    <tns:description>Location of backing services for Monitor widgets
  </tns:description>
  </tns:Endpoint>
```

```
</tns:BusinessSpaceRegistry>  
<!-- END NON-TRANSLATABLE -->
```

- Nach dem Ausführen des Befehls **installBusinessSpaceWidgets** oder **updateBusinessSpaceWidgets** müssen Sie manuelle Schritte zur Aktualisierung von Business Space-Vorlagen und -Spaces ausführen. Weitere Informationen finden Sie im Abschnitt Aktualisierung von Business Space-Vorlagen und Spaces nach der Installation oder Aktualisierung von Widgets.
- Für mehrere Instanzen von Serviceendpunkten müssen Sie die zusätzlichen Widgets für jeden zusätzlichen Cluster manuell aktivieren. Dies kann beispielsweise der Fall sein, wenn Sie Ihren vorhandenen Workload auf zwei Cluster aufteilen (partitionieren) wollen und wenn die Widgets die Daten nach Clustern unterteilt anzeigen sollen. Sie müssen beide Widgetendpunkte und die Widgetkatalogdateien bearbeiten. Weitere Informationen hierzu finden Sie im Abschnitt Business Space-Widgets für die Verwendung mehrerer Endpunkte aktivieren.
- Wenn Sie für Ihre Umgebung die Sicherheit aktiviert haben, müssen Sie sicherstellen, dass die Sicherheitsfunktion korrekt eingerichtet ist, sodass sie mit Business Space funktioniert.

### **Business Space-Widgets für die Verwendung mehrerer Endpunkte aktivieren:**

Wenn Sie eine Business Space-Instanz konfiguriert haben und eine weitere Instanz der Serviceendpunkte in Ihrer Umgebung benötigen, müssen Sie Business Space so konfigurieren, dass die Widgets Daten von mehreren Serviceendpunkten anzeigen können. Sie müssen zwei Dateien bearbeiten: Die Endpunktdatei, in der Endpunkte bei Business Space registriert werden, und die Widgetkatalogdatei, in der Widgetdefinitionen enthalten sind.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Installieren Sie das Produkt.
- Erstellen Sie einen Server oder Cluster und konfigurieren Sie ihn für Business Space.
- Konfigurieren Sie die Datenbanktabellen (bei Verwendung einer fernen Datenbank oder einer Implementierungsumgebung).
- Konfigurieren Sie die zusätzlichen REST-Services (Representational State Transfer) für Ihre zusätzlichen Widgets.

In einer Implementierungsumgebung besteht die Möglichkeit zur Aufteilung (Partitionierung) des vorhandenen Workloads. Sie können beispielsweise mit zwei Clustern arbeiten, wobei einer zur Verarbeitung der Abrechnungsdaten und der andere zur Verarbeitung der Versicherungsdaten eingesetzt wird. Ein Serviceendpunkt unterstützt jedoch immer nur einen Cluster. Um über Business Space auf beide Workloadpartitionen zugreifen zu können, müssen Sie zwei separate Widgets registrieren, die jeweils einer der Workloadpartitionen zugeordnet sind. Auf diese Weise können Sie über Business Space auf beide zugreifen. Sie können z. B. ein Widget für die Auflistung der Abrechnungsdaten zu Benutzertasks und ein Widget zur Auflistung der Daten für Versicherungstasks im Katalog haben, die beide über den gleichen Auflistungscode für Benutzertasks verfügen.

Sie müssen die Endpunktdatei und die Widgetkatalogdatei manuell bearbeiten.

Die Serviceendpunktdateien der Widgets gehören zum Lieferumfang des jeweiligen Produkts und werden während der Produktinstallation zum System hinzugefügt. Abhängig von den installierten Produkten müssen Sie eine oder auch mehrere der

Serviceendpunktdateien bearbeiten. Darüber hinaus müssen auch die in Business Space verwendeten Widgets bearbeitet werden. Die folgende Liste enthält IBM Geschäftsprozessmanagementbeispiele von Serviceendpunktdateien:

- IBM Business Monitor: `monitorEndpoints.xml`
- IBM Business Monitor mit IBM Cognos Business Intelligence: `cognosEndpoints.xml`
- WebSphere Enterprise Service Bus: `wesbWidgetEndpoints.xml` (für Widgets 'Mediationsrichtlinienverwaltung', 'Service-Browser' und 'Proxy-Gateway'), `bpmAdministrationEndpoints.xml` (für Widgets 'Verwaltung')
- IBM Business Process Manager: `wpsEndpoints.xml`, `bpmAdministrationEndpoints.xml` (für Widgets 'Verwaltung', `wesbWidgetEndpoints.xml` (für Widgets 'Mediationsrichtlinienverwaltung', 'Service-Browser' und 'Proxy-Gateway'), `HumanTaskManagementEndpoints.xml` für Business-Prozesse und Benutzertasks, `bspaceWFSEndpoints.xml` (für die Verwendung von Lotus Webform Server mit den Widgets 'Benutzertaskverwaltung').
- Alle Produkte: `wsumEndpoint.xml` (für Benutzerzugehörigkeit)

Die Widgetkatalogdateien enthalten die Definition der Widgets für Ihr Produkt. Abhängig von den installierten Produkten müssen Sie eine oder auch mehrere der folgenden Widgetdateien bearbeiten. Darüber hinaus müssen auch die in Business Space verwendeten Widgets bearbeitet werden: Die folgende Liste enthält IBM Geschäftsprozessmanagementbeispiele von Widgetkatalogdateien:

- IBM Business Monitor: `catalog_WBMonitor.xml`
- WebSphere Enterprise Service Bus: `catalogProxyGateway.xml` und `catalog_ServiceAdmin.xml`
- IBM Business Process Manager: `catalog_BPMAdministration.xml`, `catalog_BusinessRules.xml`, `catalog_ServiceAdmin.xml` und `catalog_HumanTaskManagement.xml`

Sowohl die Serviceendpunktdateien als auch die Widgetkatalogdateien befinden sich im Pfad `installationsstammverzeichnis\BusinessSpace\registryData\produktname\`. Die Endpunktdateien befinden sich im Unterverzeichnis `endpoints`, die Katalogdateien im Unterverzeichnis `catalogs`.

Das Verzeichnis `installationsstammverzeichnis\BusinessSpace\registryData\produktname\` enthält Serviceendpunkt- und Widgetkatalogschablonendateien für Ihr Produkt. Sie können die Dateien, die Sie als Schablone verwenden wollen, kopieren und Ihre Änderungen hinzufügen.

1. Um mehrere Instanzen eines Widgets zu erhalten, müssen Sie die Anwendungen installieren, die Widgets mit einem eindeutigen Anwendungsnamen und einem Stammkontext für jede Widgetinstanz zur Verfügung stellen.
  - a. Implementieren Sie die Widgetanwendung auf dem Business Space-Implementierungsziel (derselbe Server oder Cluster, auf dem die Anwendung **BSpaceEAR\_server\_knoten** ausgeführt wird) für jede Widgetinstanz. Die folgende Liste enthält IBM Geschäftsprozessmanagementbeispiele von Enterprise Archive-Dateien (EAR) für Widgets:
    - `BPMAdministrationWidgets_knotenname_servername` (für WebSphere Enterprise Service Bus und IBM Business Process Manager)
    - `HumanTaskManagementWidgets_knotenname_servername` (für IBM Business Process Manager und IBM Business Monitor)
    - `WBMDashboardWeb_knotenname_servername` (für IBM Business Monitor)

- `wesbWidgets_knotenname_servername` (für WebSphere Enterprise Service Bus)
- b. Aktualisieren Sie beim Implementieren den Anwendungsnamen und die Stammkontextnamen für Webmodule in einen eindeutigen Namen. Notieren Sie die Stammkontextnamen, die Sie verwenden.
2. Bearbeiten Sie die neuen REST-Service-Endpunkte für die zusätzlichen Anwendungsimpementierungsziele (die Server oder Cluster, in denen die REST-Service-Anwendung implementiert ist). Erstellen Sie eine Serviceendpunktdatei, um zusätzliche Serviceendpunkte hinzuzufügen.
    - a. Suchen Sie die Endpunktdateien im Verzeichnis `installationsstammverzeichnis\BusinessSpace\registryData\produktname\endpoints`. Kopieren Sie die Endpunktschablonendatei und entfernen Sie alle Endpunkte, die Sie nicht ändern möchten.
    - b. Bearbeiten Sie die Endpunktdatei und fügen Sie einen weiteren Serviceendpunkt hinzu, der mit `<tns:Endpoint>` beginnt und eine eindeutige ID (`<tns:id>`) sowie die URL für den neuen Endpunkt (`<tns:url>`) aufweist, der jedoch dieselbe Version und optional alle Ländereinstellungen so wie der ursprüngliche Endpunkt aufweist. Der Typ (`<tns:type>`) muss denselben Wert wie die ID (`<tns:id>`) aufweisen. Sie können den Namen und die Beschreibung ändern. Beispiel: My team's insurance task list (Liste der Versicherungstasks meines Teams).
    - c. Beachten Sie beim Hinzufügen von Endpunkten die folgenden Informationen:
      - `<tns:id>`: Die ID kann aus einer beliebigen Zeichenfolge bestehen, die jedoch für alle registrierten Endpunkte eindeutig sein muss. Vergewissern Sie sich, dass diese ID eindeutig ist, wenn Sie zusätzliche Endpunkte hinzufügen.
      - `<tns:type>`: Der Typ muss denselben Wert aufweisen wie `<tns:id>`.
      - `<tns:url>`: Wenn die URL-Angabe relativ ist, wird für den Serviceendpunkt davon ausgegangen, dass sich der REST-Serviceendpunkt an derselben Position wie der Business Space-Server befindet. Wenn die URL-Angabe relativ ist, stellen Sie sicher, dass die URL mit dem von Ihnen implementierten Stammkontext übereinstimmt, jedoch Anfangs- und Endanzeiger für das Verzeichnis aufweist. Beispiel: `<tns:url>/REST_Endpoint_for_server2/</tns:url>`. Falls sich Ihr Endpunkt auf einem fernen System befindet, aktualisieren Sie dieses Feld mit einer absoluten URL-Angabe mit einem Endanzeiger für das Verzeichnis.
      - `<tns:description>`: Geben Sie eine aussagekräftige Beschreibung ein, in der die Spezifik der Daten, mit denen dieser Endpunkt arbeitet, detaillierter beschrieben wird. Diese kann entweder auf dem Cluster basieren, der mit den Daten arbeitet, oder auf der Spezifik der Daten, z. B. Benutzertasks für einen Versicherungsschaden oder Benutzertasks für Abrechnungsdaten.
    - d. Speichern Sie Ihre Änderungen.

Beispiel für einen Serviceendpunkt in der Datei `monitorEndpoints.xml`:

```
<tns:Endpoint>
  <tns:id>{com.ibm.wbimonitor}monitorServiceRootId</tns:id>
  <tns:type>{com.ibm.wbimonitor}monitorServiceRootId</tns:type>
  <tns:version>1.0.0.0</tns:version>
  <tns:url>/rest/bpm/monitor/</tns:url>
  <tns:description>Location of backing services for Monitor widgets
</tns:description>
</tns:Endpoint>
```

3. Fügen Sie in der Serviceendpunktdatei einen Widgetendpunkt für jede Widgetinstanz hinzu.



- a. Bearbeiten Sie die Endpunktdatei, die Sie in Schritt 2 erstellt haben. Fügen Sie einen weiteren Widgetendpunkt hinzu, der mit `<tns:Endpoint>` beginnt und eine eindeutige ID aufweist (`<tns:id>`). Der Typ (`<tns:type>`) muss denselben Wert wie die ID (`<tns:id>`) aufweisen. Die URL für den neuen Endpunkt (`<tns:url>`) sollte mit dem Stammkontext übereinstimmen, den Sie in Schritt 1 implementiert haben, jedoch Anfangs- und Endanzeiger für das Verzeichnis aufweisen. Beispiel: `<tns:url>/BspaceWidgetsWPS2/</tns:url>`. Der von Ihnen hinzugefügte Widgetendpunkt sollte dieselbe Version enthalten und kann optional alle Ländereinstellungen des ursprünglichen Endpunkts enthalten. Sie können den Namen und die Beschreibung ändern.
- b. Beachten Sie beim Hinzufügen von Endpunkten die folgenden Informationen:
  - `<tns:id>`: Die ID kann aus einer beliebigen Zeichenfolge bestehen, die jedoch für alle registrierten Endpunkte eindeutig sein muss. Vergewissern Sie sich, dass diese ID eindeutig ist, wenn Sie zusätzliche Endpunkte hinzufügen.
  - `<tns:type>`: Der Typ muss denselben Wert aufweisen wie `<tns:id>`.
  - `<tns:url>`: Stellen Sie für den Widgetendpunkt sicher, dass die URL mit dem von Ihnen implementierten Stammkontext übereinstimmt, jedoch Anfangs- und Endanzeiger für das Verzeichnis aufweist. Beispiel: `<tns:url>/BspaceWidgetsWPS2/</tns:url>`.
  - `<tns:description>`: Geben Sie eine aussagekräftige Beschreibung ein, in der die Spezifik der Daten, mit denen dieser Endpunkt arbeitet, detaillierter beschrieben wird. Diese kann entweder auf dem Cluster basieren, der mit den Daten arbeitet, oder auf der Spezifik der Daten, z. B. Benutzertasks für einen Versicherungsschaden oder Benutzertasks für Abrechnungsdaten.
- c. Speichern Sie Ihre Änderungen.

Beispiel für einen Widgetendpunkt in der Datei `monitorEndpoints.xml`:

```
<tns:Endpoint>
<tns:id>{com.ibm.wbimonitor}monitorWidgetRootId2</tns:id>
  <tns:type>{com.ibm.wbimonitor}monitorWidgetRootId2</tns:type>
  <tns:version>1.0.0</tns:version>
  <tns:url>/BusinessDashboards/</tns:url>
  <tns:description>Location for Monitor widgets</tns:description>
</tns:Endpoint>
```

4. Erstellen Sie eine Widgetkatalogdatei und fügen Sie neue Widgetdefinitionen hinzu.
  - a. Suchen Sie die Widgetkatalogdatei im Verzeichnis `installationsstammverzeichnis\BusinessSpace\registryData\produktname\catalogs`. Kopieren Sie die Katalogschablonendatei. Verwenden Sie folgenden Standard für den neuen Dateinamen: `catalog_widget.xml` (ohne Leerzeichen im Dateinamen) wobei `widget` dem ID-Wert für das Element `<catalog>` in der Datei entspricht. Entfernen Sie alle `<category>`-Elemente, die Sie nicht ändern möchten. Entfernen Sie für die Kategorie, mit der Sie arbeiten möchten, alle `<entry>`-Elemente, die Sie nicht ändern möchten.
  - b. Fügen Sie einen Eintrag (`<entry>`) mit einer eindeutigen ID, beispielsweise `id="{com.ibm.bspace.widget}widget_id`, und mit einem eindeutigen Namen, beispielsweise `unique-name="{com.ibm.bspace.widget}widgetname`, hinzu. Sie können alle anderen Definitionen beibehalten.
  - c. Ändern Sie den Titel und die Beschreibung, um das neue Widget in Business Space als separates Widget bereitzustellen, in dem die Spezifik des neuen Endpunkts definiert ist. Sie können dem Widget beispielsweise im Titel (`<title>`) den Namen `My team's insurance task list` zuordnen. Der Ti-



tel soll dem Geschäftsbenutzer die Auswahl des richtigen Widgets erleichtern. Die Beschreibung soll dem Geschäftsbenutzer das Verständnis der Datenspezifik und der Funktionalität des Widgets erleichtern, das von ihnen ausgewählt wird.

- d. Bearbeiten Sie die neue XML-Widgetkatalogdatei, um auf den neuen Widgetendpunkt zu verweisen. Ändern Sie die Definition, damit sie mit `<tns:id>` des Widgetendpunkts übereinstimmt, den Sie in Schritt 3.a hinzugefügt haben.

Ändern Sie zum Beispiel in: ...

```
<definition>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId2/com/ibm/wbimonitor/common/iWidgets/instances_iWidget.xml</definition>
```

...

- e. Stellen Sie in den Metadaten (`<metadata>`) der Katalogdatei sicher, dass der Endpunkt (`endpoint://`) mit dem Typ und der ID in der Endpunktdatei (`<tns:type>` und `<tns:id>`) übereinstimmt.
- f. Stellen Sie in den Metadaten (`<metadata>`) der Katalogdatei sicher, dass die Referenzversion "refVersion" : mit der Version in der Endpunktdatei (`<tns:version>`) übereinstimmt.
- g. Speichern Sie Ihre Änderungen.

Sie können die Widgetdefinition im unten dargestellten Codeausschnitt als Grundlage für Ihre Änderungen verwenden::

```
<entry id="{com.ibm.wbimonitor}instances"
unique-name="{com.ibm.wbimonitor}instances">
  <title>
    <!-- END NON-TRANSLATABLE -->
    <nls-string xml:lang="en">Instances</nls-string>
    <!-- START NON-TRANSLATABLE -->
  </title>
  <description>
    <!-- END NON-TRANSLATABLE -->
    <nls-string xml:lang="en">Instances</nls-string>
    <!-- START NON-TRANSLATABLE -->
  </description>
  <shortDescription>
    <!-- END NON-TRANSLATABLE -->
    <nls-string xml:lang="en">This widget displays a dashboard with
the available monitoring context in either individual instances or user-
defined groups of context instances.</nls-string>
    <!-- START NON-TRANSLATABLE -->
  </shortDescription>
  <definition>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId
/com/ibm/wbimonitor/common/iWidgets/instances_iWidget.xml</definition>
  <content>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
thumb_instances.gif</content>
  <preview>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
prev_instances.gif</preview>
  <previewThumbnail>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/
img/prev_instances.gif</previewThumbnail>
  <help>endpoint://{com.ibm.bspace}bSpaceWidgetHelpRootId/topic/
com.ibm.bspace.help.widg.mon.doc/topics/help_instance_whatIs.html</help>
  <icon>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
icon_instances.gif</icon>
  <metadata name="com.ibm.mashups.builder.autoWiringEnabled">true
</metadata>
  <metadata name="com.ibm.bspace.version">7.0.0.0</metadata>
  <metadata name="com.ibm.bspace.owner">International Business
Machines Corp.</metadata>
  <metadata name="com.ibm.bspace.serviceEndpointRefs">
[{"name":"serviceUrlRoot", "required":"true",
"refId":"endpoint://{com.ibm.wbimonitor}monitorServiceRootId",
"refVersion":"1.0.0.0"}]</metadata>
</entry>
```

5. Komprimieren Sie die neue Serviceendpunktdatei und die neue Katalogdatei in einer Datei und führen Sie den Befehl **updateBusinessSpaceWidgets** mit dem Parameter **-widgets** aus, um die Position der komprimierten Datei anzugeben.
  - Nach dem Ausführen des Befehls **updateBusinessSpaceWidgets** müssen Sie manuelle Schritte ausführen, um die Business Space-Schablonen und -Spaces zu ak-

tualisieren. Weitere Informationen finden Sie im Abschnitt Aktualisierung von Business Space-Vorlagen und Spaces nach der Installation oder Aktualisierung von Widgets.

- Wenn Business Space in einer anderen Zelle als die REST-Services ausgeführt wird, müssen Sie die Endpunktdateien manuell bearbeiten.
- Wenn Sie für Ihre Umgebung die Sicherheit aktiviert haben, müssen Sie sicherstellen, dass die Sicherheitsfunktion korrekt eingerichtet ist, sodass sie mit Business Space funktioniert.

### Widgets für mehrere Produkte konfigurieren:

Mit dem Befehl **installBusinessSpaceWidgets** können Sie Business Space-Widgets für ein Produkt in einem Business Space konfigurieren oder ihm hinzufügen, selbst wenn der Business Space bereits mit einem anderen Produkt konfiguriert wurde.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Führen Sie alle Schritte zum Installieren und Konfigurieren eines Produkts aus und konfigurieren Sie Business Space.
- Führen Sie alle Schritte zum Installieren und Konfigurieren des zusätzlichen Produkts aus.

Sie können mehrere Produkte für die Verwendung mit Business Space installieren und die Widgets für beide Produkte nach der Installation des zweiten Produkts konfigurieren. Wenn Sie aber ein zweites Produkt installieren, nachdem Sie Business Space mit den Widgets für das erste Produkt bereits konfiguriert haben, müssen Sie den Befehl **installBusinessSpaceWidgets** verwenden und damit die Widgets für das zweite Produkt hinzufügen oder konfigurieren, sodass sie mit demselben Business Space funktionieren.

In einer eigenständigen Erweiterung werden Widgets automatisch installiert. Beispielsweise werden Widgets installiert, wenn Sie ein eigenständiges IBM Business Process Manager-Profil erstellen, den Server für Business Space konfigurieren, IBM Business Monitor installieren und den bereits konfigurierten Server auf IBM Business Monitor erweitern.

1. Stellen Sie sicher, dass das Deployment Manager-Profil betriebsbereit ist und öffnen Sie unter diesem Profil ein Befehlsfenster.  
Der Befehl 'wsadmin' befindet sich im Verzeichnis `profiles/profilname/bin`.
2. Geben Sie an der Eingabeaufforderung **wsadmin** ein, um die **wsadmin**-Umgebung zu starten.
3. Verwenden Sie den Befehl **installBusinessSpaceWidgets**, um bestimmte Widgets, die sich im Verzeichnis `installationsstammverzeichnis/BusinessSpace/registryData/produktname/widgets` befinden, zu installieren, zu implementieren und zu registrieren.

Im folgenden Beispiel wird mit Jython der Befehl **installBusinessSpaceWidgets** ausgeführt, um Widgets für IBM Business Monitor zu installieren, die mit der zuvor für IBM Business Process Manager konfigurierten Business Space-Umgebung verwendet werden.

```
AdminTask.installBusinessSpaceWidgets(['-nodeName knotenname  
-serverName servername -widgets  
installationsstammverzeichnis/BusinessSpace/registryData/WBM/widgets/Widgets_WBMonitor.zip'])
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask installBusinessSpaceWidgets {-nodeName knotenname  
-serverName servername -widgets  
installationsstammverzeichnis/BusinessSpace/registryData/WBM/widgets/prWidgets_WBMonitor.zip}
```

Führen Sie nach der Konfiguration der Widgets die folgenden Schritte aus, um Business Space für die Laufzeitumgebung zu aktivieren:

- Führen Sie nach dem Ausführen des Befehls **installBusinessSpaceWidgets** oder **updateBusinessSpaceWidgets** manuelle Schritte zur Aktualisierung von Business Space-Vorlagen und -Spaces aus. Weitere Informationen finden Sie im Abschnitt Aktualisierung von Business Space-Vorlagen und Spaces nach der Installation oder Aktualisierung von Widgets.
- Konfigurieren Sie REST-Services. Weitere Informationen hierzu finden Sie im Abschnitt REST-Services konfigurieren.
- Registrieren Sie die REST-Endpunkte. Weitere Informationen hierzu finden Sie im Abschnitt "Business Space konfigurieren und REST-Endpunkte in der Administrationskonsole konfigurieren".
- Überprüfen Sie, ob die Sicherheitsfunktion korrekt eingerichtet ist, sodass sie mit Business Space und den von Ihrem Team verwendeten Widgets funktioniert. Weitere Informationen enthält der Abschnitt Sicherheit für Business Space konfigurieren.

## Bestimmte Widgets in Business Space einrichten

Für einige der im Lieferumfang Ihres Produkts enthaltenen Widgets sind zusätzliche Konfigurationsschritte für die Verwendung in Business Space erforderlich.

Ihr Geschäftsprozessmanagementprodukt enthält mehrere Widgets, von denen einige zusätzlich konfiguriert werden müssen, um über Business Space mit Ihrer Lösung kommunizieren zu können.

### Service-Monitor konfigurieren:

Wenn Sie einen neuen Server erstellen und mit dem Widget 'Service-Monitor' in Business Space die Antwortzeit und den Durchsatz der Anforderungsverarbeitung für die von einem SCA-Modul bereitgestellten oder aufgerufenen Services messen wollen, müssen Sie in der Administrationskonsole die Serviceüberwachung konfigurieren und aktivieren.

**Erforderliche Sicherheitsrolle für diese Task:** Wenn die Verwaltungssicherheit aktiviert ist, müssen Sie zum Ausführen dieser Task als Administrator angemeldet sein.

Der Service-Monitor-Server muss aktiviert werden, bevor das Widget 'Service-Monitor' verwendet werden kann. In eigenständigen Serverumgebungen wird der Service-Monitor-Server standardmäßig bei der Profilerstellung aktiviert. In Implementierungsumgebungen und bei neuen Servern, die mit der Administrationskonsole erstellt wurden, müssen Sie den Service-Monitor-Server manuell über die Administrationskonsole aktivieren. Bei Topologiemustern des Typs 'Remote Messaging und Fernunterstützung' muss der Service-Monitor-Server im Unterstützungskluster aktiviert werden; bei Mustern des Typs 'Remote Messaging, Fernunterstützung und Web (4 Cluster)' muss der Server im Webcluster aktiviert werden.

Der Service-Monitor besitzt eine Client/Server-Architektur.

- Der Service-Monitor-Agent erfasst den Durchsatz und die Antwortzeit von Operationen und sendet die erfassten Messwertdaten zum Service-Monitor-Server.

- Der Service-Monitor-Server erfasst und verarbeitet Messwerte für Antwortzeit und Durchsatz von allen aktiven Service-Monitor-Agenten, um daraus Statistiken zu berechnen und diese zu speichern.

**Wichtig:** Wenn Sie einen externen HTTP-Server verwenden, um auf Business Space zuzugreifen, stellen Sie sicher, dass der HTTP-Server für codierte Schrägstriche konfiguriert ist. Details hierzu finden Sie in der Dokumentation des HTTP-Servers.

1. Melden Sie sich als Administrator bei der Administrationskonsole an.
2. Konfigurieren Sie den Service-Monitor-Server.
  - a. Klicken Sie in der Konsole auf **Server > Servertypen > WebSphere-Anwendungsserver > *servername* > Service-Monitor**.
  - b. Klicken Sie auf der Seite 'Service-Monitor' auf **Service-Monitor aktivieren**.
  - c. Prüfen Sie die standardmäßigen Grenzwerte der Puffer- und Abfragegröße des Service-Monitors und ändern Sie sie gegebenenfalls.
  - d. Geben Sie die Ziele der Serviceüberwachung an. Dies sind die Service-Monitor-Agenten, von denen Sie Daten erfassen wollen.

Tabelle 7. Überwachung

Zu überwachende Ziele	Auszuführende Schritte
Alle aktiven Service-Monitor-Agenten überwachen	Stellen Sie sicher, dass die Option <b>Alle Service-Monitor-Agenten aktivieren</b> ausgewählt ist.
Eine bestimmte Teilmenge der aktiven Service-Monitor-Agenten überwachen	<ol style="list-style-type: none"> <li>1. Inaktivieren die Option <b>Alle Service-Monitor-Agenten aktivieren</b>. Eine Tabelle mit Objektgruppen wird angezeigt. Bei einer neuen Konfiguration ist die Tabelle leer.</li> <li>2. Klicken Sie auf <b>Hinzufügen</b>. Die Seite 'Implementierungsziel auswählen' wird geöffnet.</li> <li>3. Wählen Sie auf der Seite 'Implementierungsziel auswählen' in der Objektgruppentabelle das Implementierungsziel aus, dessen Agent Sie überwachen wollen.</li> <li>4. Klicken Sie auf <b>OK</b>, um zur Seite 'Service-Monitor-Server' zurückzukehren.</li> <li>5. Wiederholen Sie die Schritte 2 bis 4, bis Sie alle Agenten hinzugefügt haben, die Sie überwachen wollen.</li> </ol>

- e. Klicken Sie auf der Seite 'Service-Monitor-Server' auf **OK**. Die Konfiguration wird gespeichert und wird sofort wirksam.
3. Konfigurieren Sie den Service-Monitor-Agenten.
    - a. Klicken Sie in der Konsole auf **Server > Servertypen > WebSphere-Anwendungsserver > *servername* > Service-Monitor-Agent**.
    - b. Klicken Sie auf der Seite 'Service-Monitor-Agent' auf **Service-Monitor-Agenten aktivieren**.
    - c. Prüfen Sie die Standardwerte der Agentenkonfiguration und ändern Sie sie gegebenenfalls.
    - d. Klicken Sie auf **OK**.

## Standard-Business Space unter z/OS installieren:

Unter den meisten Betriebssystemen wird der Standard-Business Space automatisch installiert. Für z/OS-Systeme, die die lokale Benutzerregistry des Betriebssystems und die SAF-Berechtigung verwenden, müssen einige zusätzliche Schritte ausgeführt werden, um den Standard-Business Space zu installieren.

Business Space verwendet den primären Benutzernamen mit Verwaltungsaufgaben zur Festlegung des Administrators für den Eingangsbereich. Unter z/OS gibt es jedoch das Konzept eines primären Administrators nicht, wenn die lokale Benutzerregistry des Betriebssystems und die SAF-Berechtigung verwendet werden. Dies bedeutet, dass Sie eine gültige ID in der Registry für die Installation des Standardbereichs angeben müssen.

- **Eigenständiger Server:**

1. Ändern Sie die Eigenschaft **MashupAdminForOBSpace** in der Konfigurationsdatei `profilstammverzeichnis/BusinessSpace/knotenname/servername/mm.runtime.prof/config/ConfigService.properties` durch die Angabe einer gültigen Benutzer-ID.
2. Führen Sie den Befehl **updatePropertyConfig** in der 'wsadmin'-Umgebung des Profils aus:  

```
$AdminTask updatePropertyConfig {-serverName servername -nodeName knotenname -propertyFileName
```
3. Führen Sie `$AdminConfig save` aus.
4. Öffnen Sie in dem Profil, in dem sich der Server befindet, die Datei `profilstammverzeichnis/BusinessSpace/knotenname/servername/mm.runtime.prof/public/oobLoadedStatus.properties` und aktualisieren Sie die Eigenschaft **importSpaces.txt**:  

```
importSpaces.txt=true
```
5. Führen Sie einen Neustart des Servers aus.

- **Cluster:**

1. Ändern Sie die Eigenschaft **MashupAdminForOBSpace** in der Konfigurationsdatei `deployment_manager-profilstammverzeichnis/BusinessSpace/clustername/mm.runtime.prof/config/ConfigService.properties` durch die Angabe einer gültigen Benutzer-ID.
2. Führen Sie den Befehl **updatePropertyConfig** in der 'wsadmin'-Umgebung des Deployment Manager-Profiles aus:  

```
$AdminTask updatePropertyConfig {-clusterName clustername -propertyFileName "profilstammverz
```
3. Führen Sie `$AdminConfig save` aus.
4. Ermitteln Sie den Namen der Zelle, des Knotens und des Servers für das angepasste Profil:
  - a. Öffnen Sie im Deployment Manager-Profil die Datei `stammverzeichnis_des_deployment_manager-profilstammverzeichnis/BusinessSpace/cluster_name/mm.runtime.prof/config/ConfigService.properties`.
  - b. Suchen Sie in den Eigenschaften **com.ibm.mashups.directory.templates** oder **com.ibm.mashups.directory.spaces** nach den Namen für Zelle, Knoten und Server.
  - c. Verwenden Sie die Namen von Zelle, Knoten und Server, um das benutzerdefinierte Profil zu suchen.
5. Öffnen Sie im benutzerdefinierten Profil die Datei `stammverzeichnis_des_benutzerdefinierten_profilstammverzeichnis/BusinessSpace/clustername/mm.runtime.prof/public/oobLoadedStatus.properties` und aktualisieren Sie die Eigenschaft **importSpaces.txt**:  

```
importSpaces.txt=true
```

6. Resynchronisieren Sie das benutzerdefinierte Profil:
  - a. Öffnen Sie die Administrationskonsole und klicken Sie auf **Systemadministration > Knoten**.
  - b. Klicken Sie auf **Vollständige Neusynchronisation**.
7. Starten Sie das Cluster erneut.

## Sicherheitsfunktion für Business Space einrichten

Wenn Sie Business Space powered by WebSphere in Ihrer Umgebung verwenden, müssen Sie die Sicherheitsoptionen festlegen, die angeben, wie Ihr Team in Business Space mit Artefakten arbeiten wird. Wenn Sie die Sicherheit für Business Space aktivieren möchten, konfigurieren Sie die Anwendungssicherheit und legen Sie ein Benutzerrepository fest. Weisen Sie eine Superuser-Rolle zu, um Business Space-Administratoren zu definieren.

Aktivieren Sie für ein optimales Ergebnis die Sicherheit, bevor Sie Business Space konfigurieren. Wenn Sie die Sicherheit später aktivieren, verwenden Sie auf der Administrationskonsole die Seite für die Verwaltung der globalen Sicherheit, um die Verwaltungssicherheit und die Anwendungssicherheit zu aktivieren. Auf derselben Seite der Administrationskonsole können Sie auch ein Benutzeraccount-Repository angeben und Sie können die Standardoption für eingebundene Repositories in ein anderes Benutzerrepository ändern. Um anzugeben, welche Benutzer Business Space-Administratoraktionen in der Business Space-Umgebung ausführen können, ordnen Sie die Business Space-Superuser-Rolle zu. Für Ihre Umgebung kann aber auch eine andere Sicherheitskonfiguration erforderlich sein.

**Wichtig:** Standardmäßig schränkt die Ajax-Proxy-Konfiguration, die mit Business Space-Widgets verwendet wird, den Zugriff auf IP-Adressen nicht ein. Die standardmäßig offene Konfiguration des Ajax-Proxys bietet nicht die für Produktionsszenarios erforderliche Sicherheit. Um den Ajax-Proxy so zu konfigurieren, dass er nur Inhalte von bestimmten Sites anzeigt oder Inhalte von bestimmten Sites blockiert, führen Sie die Schritte aus, die unter IP-Adressen mit dem Business Space-Ajax-Proxy blockieren beschrieben sind.

### Sicherheit für Business Space aktivieren:

Falls eine gesicherte Umgebung verwendet werden soll, aktivieren Sie die Sicherheit, bevor Sie Business Space konfigurieren. Bei Bedarf können Sie die Sicherheitsfunktion später aber auch manuell aktivieren. Um die Sicherheitsfunktion für Business Space einzuschalten, müssen Sie sowohl die Anwendungssicherheitsfunktion als auch die Funktion für die administrative Sicherheit aktivieren.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Überprüfen der Registrierung Ihrer Benutzer-ID in der Benutzerregistry Ihres Produkts.

Business Space ist vorkonfiguriert, um die Authentifizierung und die Berechtigung des Zugriffs sicherzustellen. Beim Zugriff auf Business Space werden die Benutzer aufgefordert, sich zu authentifizieren. Nicht authentifizierte Benutzer werden auf eine Anmeldeseite umgeleitet.

Standardmäßig ist Business Space für den Zugriff über HTTPS konfiguriert. Wenn Sie HTTP-Verbindungen bevorzugen, da Ihr System sich sowieso hinter einer Firewall befindet, können Sie auf HTTP umschalten, indem Sie das Script `configBspaceTransport.py` ausführen. Das Script `configBspaceTransport.py` enthält



Parameter, mit denen Sie wahlweise auf HTTP oder HTTPS umschalten können, falls Sie eine frühere Einstellung ändern möchten. Siehe HTTP- oder HTTPS-Einstellungen für Business Space festlegen.

Um den authentifizierten Zugriff auf Business Space zu ermöglichen, müssen Sie auf Ihrem System eine Benutzerregistry konfiguriert und die Funktion für die Anwendungssicherheit aktiviert haben. Die Vergabe der Berechtigung für den Inhalt von Speicherbereichen und Seiten in Business Space wird in Business Space intern im Rahmen der Speicherbereichsverwaltung durchgeführt.

1. Vollständige Anweisungen zur Sicherheit finden Sie in der Dokumentation zur Sicherheitsfunktion Ihres Produkts.
2. Für die Business Space-Anwendung müssen Sie auf der Seite **Globale Sicherheit** der Administrationskonsole sowohl **Verwaltungssicherheit aktivieren** als auch **Anwendungssicherheit aktivieren** auswählen.
3. Wenn Sie die Sicherheit nach dem Konfigurieren von Business Space mit Ihrem Profil aktivieren oder entfernen wollen, müssen Sie die Eigenschaft `noSecurityAdminInternalUserOnly` in der Datei `ConfigServices.properties` ändern.

Die Eigenschaft `noSecurityAdminInternalUserOnly` gibt die Business Space-Administrator-ID an, wenn die Sicherheit inaktiviert ist. Standardmäßig wird die Eigenschaft in der Business Space-Konfiguration auf **BPMAdministrator** gesetzt, wenn die Sicherheit inaktiviert ist. Bei aktivierter Sicherheit wird diese Eigenschaft standardmäßig auf die Anwendungsserver-Administrator-ID gesetzt. Wenn Sie die Sicherheit nach dem Konfigurieren von Business Space aktivieren oder entfernen wollen, verwenden Sie die Anwendungsserver-Administrator-ID.

- a. Ändern Sie die Eigenschaft `noSecurityAdminInternalUserOnly` in Datei `ConfigServices.properties` und stellen Sie sie auf die Anwendungsserver-Administrator-ID ein. Die Datei `ConfigServices.properties` befindet sich bei einem eigenständigen Server im Pfad `stammverzeichnis_des_profils\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties` und bei einem Cluster im Pfad `stammverzeichnis_des_deployment_manager-profils\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties`.
- b. Führen Sie den Befehl **updatePropertyConfig** mit dem `wsadmin`-Scripting-Client aus.

**Wichtig:** Für Windows muss der Wert für den Parameter **propertyFileName** der vollständige Pfad zu der Datei sein, und alle Backslashes müssen doppelt angegeben werden. Beispiel: `AdminTask.updatePropertyConfig(['-serverName servername -nodeName knotenname -propertyFileName "profilstammverzeichnis\\BusinessSpace\\knotenname\\servername\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"'])`.

- Eigenständiger Server:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig(['-serverName servername -nodeName knotenname
-propertyFileName "profilstammverzeichnis\BusinessSpace\knotenname\servername
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"'])
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-serverName servername -nodeName knotenname
-propertyFileName "profilstammverzeichnis\BusinessSpace\knotenname\servername
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

- Cluster:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-clusterName clustername -propertyFileName
"deployment_manager-profilstammverzeichnis\BusinessSpace\clustername\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"]')
```

```
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-clusterName clustername -propertyFileName
"deployment_manager-profilstammverzeichnis\BusinessSpace\clustername\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

c. Starten Sie den Server erneut.

d. Melden Sie sich bei Business Space an und ordnen Sie die Eigner der Standard-Spaces der neuen Administrator-ID zu.

- Nachdem die Funktion für die administrative Sicherheit sowie für die Anwendungssicherheit aktiviert wurde, erhalten Sie eine Aufforderung zur Eingabe einer Benutzer-ID und des zugehörigen Kennworts, wenn Sie sich bei Business Space anmelden. Zur Anmeldung müssen Sie dann eine gültige Benutzer-ID und das zugehörige Kennwort aus der ausgewählten Benutzerregistry verwenden. Nach dem Aktivieren der Funktion für die administrative Sicherheit müssen Sie sich beim Zurückkehren zur Administrationskonsole jedes Mal mit der Benutzer-ID anmelden, die über Administratorberechtigung verfügt.
- Wenn Sie für das Benutzeraccount-Repository ein anderes als das Standardrepository für Ihr Produktprofil angeben möchten, führen Sie die Schritte aus, die unter Benutzeraccount-Repository auswählen für Business Space beschrieben sind.
- Wenn Sie mit einer zellenübergreifenden Umgebung arbeiten, in der Business Space an einer anderen Position ausgeführt wird als Ihr Produkt, und wenn sich die Knoten nicht in derselben Zelle befinden, richten Sie SSO- und SSL-Zertifikate ein (Single Sign-on, Secure Sockets Layer). Folgen Sie den Anweisungen im Thema SSO und SSL für Business Space einrichten.
- Um anzugeben, welche Benutzer Business Space-Administratoraktionen in der Business Space-Umgebung ausführen können, siehe Business Space-Superuser-Rolle zuordnen.

### Benutzerrepository für Business Space auswählen:

Die Option für eingebundene Repositories ist die Standardoption für Benutzeraccount-Repositories bei Profilen. Sie können den Typ Ihres Benutzeraccount-Repositories ändern, wenn Ihre Umgebung dies erfordert.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Aktivieren der Anwendungssicherheit und Verwaltungssicherheit. Vgl. „Sicherheit für Business Space aktivieren“ auf Seite 280.
- Überprüfen der Registrierung Ihrer Benutzer-ID in der Benutzerregistry Ihres Produkts.

Um den authentifizierten Zugriff auf Business Space zu ermöglichen, müssen Sie auf Ihrem System eine Benutzerregistry konfiguriert und die Funktion für die Anwendungssicherheit aktiviert haben. Weitere Informationen zur Anwendungssicherheit finden Sie in „Sicherheit für Business Space aktivieren“ auf Seite 280.

Besonderheiten bei der Verwendung einer Benutzeraccount-Registry mit Business Space:

- Je nach Typ der von Ihnen verwendeten LDAP-Konfiguration können Ihre Einstellungen Ihre Fähigkeit beeinträchtigen, auf Business Space korrekt zuzugreifen. Stellen Sie sicher, dass die Benutzerfilter, Gruppenfilter und Zuordnungseinstellungen ordnungsgemäß konfiguriert sind. Weitere Informationen zu diesem Thema finden Sie im Abschnitt LDAP-Suchfilter konfigurieren in der Dokumentation von WebSphere Application Server.
  - Je nach Typ der von Ihnen verwendeten Konfiguration für eingebundene Repositories können Ihre Einstellungen Ihre Fähigkeit beeinträchtigen, auf Business Space korrekt zuzugreifen. Stellen Sie sicher, dass die Realms ordnungsgemäß konfiguriert sind. Weitere Informationen zu diesem Thema finden Sie im Abschnitt Realm in einer Konfiguration für eingebundene Repositories verwalten in der Dokumentation von WebSphere Application Server.
  - Die LDAP-Sicherheit ist standardmäßig so eingerichtet, dass die Anmeldeeigenschaft `uid` (Benutzer-ID) für die Suche in Business Space verwendet wird. Wenn Ihre LDAP-Sicherheit so geändert wird, dass für die Anmeldeeigenschaft ein anderes eindeutiges LDAP-Feld verwendet wird (beispielsweise `mail` (E-Mail-Adresse)), müssen Sie die Eigenschaft `userIdKey` in der Datei `ConfigServices.properties` ändern, damit die Suche in Business Space funktioniert. Führen Sie Schritt 3 unten aus.
  - Stellen Sie bei Verwendung einer Microsoft SQL Server-Datenbank und der Option **Eigenständige LDAP-Registry** sicher, dass der Benutzer-DN nicht länger als 450 Zeichen ist. Sollten einige Benutzer-DN-Einträge 450 Zeichen überschreiten, müssen Sie die Option **Eingebundene Repositories** für das Benutzeraccount-Repository festlegen.
  - Wenn Sie **Eingebundene Repositories** verwenden, verfügen Sie in Ihren Widgets und dem Framework über zusätzliche Funktionen wie beispielsweise erweiterte Suchfunktionen. Bei der Suche nach Benutzern für die gemeinsame Nutzung von Speicherbereichen und Seiten umfasst der Suchbereich auch die E-Mail-Adresse sowie den vollständigen Benutzernamen und die Benutzer-ID.
1. Auf der Seite **Globale Sicherheit** der Administrationskonsole können Sie unter **Benutzeraccount-Repository** entweder **Eingebundene Repositories**, **Lokales Betriebssystem**, **Eigenständige LDAP-Registry** oder **Eigenständige benutzerdefinierte Registry** festlegen.
  2. Starten Sie den Server erneut.
  3. Wenn Sie die Standardeinstellung **Eingebundene Repositories** des Standardbenutzerrepositorys ändern wollen, modifizieren Sie die Eigenschaft `MashupAdminFor00Bspace` in `ConfigServices.properties` so, dass die richtige Benutzer-ID (die UID-Eigenschaft für Ihr Benutzerrepository) als gültige Administrator-ID definiert wird.
    - a. Kopieren Sie die geänderte Datei in einen leeren Ordner auf Ihrem System. Die Datei `ConfigServices.properties` befindet sich bei einem eigenständigen Server im Pfad `stammverzeichnis_des_profils\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties` und bei einem Cluster im Pfad `stammverzeichnis_des_deployment_manager_profils\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties`.
    - b. Führen Sie den Befehl **updatePropertyConfig** mit dem `wsadmin`-Scripting-Client aus.

**Wichtig:** Für Windows muss der Wert für den Parameter **propertyFileName** der vollständige Pfad zu der Datei sein, und alle Backslashes müssen dop-

pelt angegeben werden. Beispiel: `AdminTask.updatePropertyConfig('[-serverName servername -nodeName knotenname -propertyFileName "profilstammverzeichnis\\BusinessSpace\\knotenname\\servername\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')`.

- Eigenständiger Server:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-serverName servername -nodeName knotenname
-propertyFileName "profilstammverzeichnis\\BusinessSpace\\knotenname\\servername
\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-serverName servername -nodeName knotenname
-propertyFileName "profilstammverzeichnis\\BusinessSpace\\knotenname\\servername
\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

- Cluster:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-clusterName clustername -propertyFileName
"deployment_manager-profilstammverzeichnis\\BusinessSpace\\clustername\\mm.runtime.prof\\
config\\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-clusterName clustername -propertyFileName
"deployment_manager-profilstammverzeichnis\\BusinessSpace\\clustername\\mm.runtime.prof\\
config\\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

- Melden Sie sich bei Business Space an und ordnen Sie die Eigner der Standard-Spaces der neuen Administrator-ID zu.
- Wenn Sie ein LDAP-Repository mit einem eindeutigen LDAP-Feld verwenden (z. B. mail (E-Mail-Adresse) für die Anmeldeeigenschaft anstelle von uid (Benutzer-ID)), ändern Sie die Eigenschaft `userIdKey` in der Datei `ConfigServices.properties`, damit die Suche in Business Space funktioniert.
    - Lokalisieren Sie die Datei `ConfigServices.properties` bei einem eigenständigen Server im Pfad `stammverzeichnis_des_profils\\BusinessSpace\\knotenname\\servername\\mm.runtime.prof\\config\\ConfigService.properties` und bei einem Cluster im Pfad `stammverzeichnis_des_deployment_manager_profils\\BusinessSpace\\clustername\\mm.runtime.prof\\config\\ConfigService.properties`.
    - Ändern Sie das Attribut `userIdKey` von `uid` so, dass es mit der Anmeldeeigenschaft für Ihr LDAP-Benutzerrepository übereinstimmt, beispielsweise in `mail`.
    - Kopieren Sie die geänderte Datei in einen leeren Ordner auf Ihrem System.
    - Führen Sie den Befehl **updatePropertyConfig** mit dem `wsadmin`-Scripting-Client aus.

**Wichtig:** Für Windows muss der Wert für den Parameter **propertyFileName** der vollständige Pfad zu der Datei sein, und alle Backslashes müssen doppelt angegeben werden. Beispiel: `AdminTask.updatePropertyConfig('[-serverName servername -nodeName knotenname -propertyFileName "profilstammverzeichnis\\BusinessSpace\\knotenname\\servername\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')`.

- Eigenständiger Server:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-serverName servername -nodeName knotenname
-propertyFileName "profilstammverzeichnis\BusinessSpace\knotenname\servername
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-serverName servername -nodeName knotenname
-propertyFileName "profilstammverzeichnis\BusinessSpace\knotenname\servername
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

- Cluster:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-clusterName clustername -propertyFileName
"deployment_manager-profilstammverzeichnis\BusinessSpace\clustername\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-clusterName clustername -propertyFileName
"deployment_manager-profilstammverzeichnis\BusinessSpace\clustername\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

5. Wenn Sie die Anmeldung bei Business Space auf eine Untergruppe von Benutzern und Gruppen beschränken möchten, können Sie die Business Space Java EE-Sicherheitsrolle ändern.
  - a. Aktualisieren Sie die Zuordnung zu Benutzern/Gruppen für zwei Enterprise-Anwendungen: **BSpaceEAR\_knoten\_server** und **mm.was\_knoten\_server** (für eine eigenständige Serverumgebung) oder **BSpaceEAR\_cluster** und **mm.was\_cluster** (für eine Network Deployment-Umgebung).
  - b. Klicken Sie auf **Anwendungen > Anwendungstypen > WebSphere-Enterprise-Anwendungen** und wählen Sie die zwei Anwendungen aus.
  - c. Wählen Sie im rechten Fenster unter 'Detaileigenschaften' die Option **Zuordnung von Sicherheitsrollen zu Benutzern/Gruppen** aus.
  - d. Ordnen Sie die Rollen **businessspaceusers** und **Allauthenticated** der zwei Anwendungen erneut zu, indem Sie zuerst das Sondersubjekt entfernen.
  - e. Klicken Sie auf die Option **Sondersubjekte zuordnen** und wählen Sie **Keine** aus.
  - f. Klicken Sie auf die Option **Benutzer zuordnen** oder **Gruppen zuordnen** und ordnen Sie jede Rolle Ihren ausgewählten Benutzern oder Gruppen zu.

Beachten Sie, dass die Änderung der Java EE-Sicherheitsrollenzuordnung die Suchfunktion für Benutzer/Gruppen in Business Space nicht beeinflusst.

6. Starten Sie den Server erneut.
7. Melden Sie sich bei Business Space an und ordnen Sie die Eigner der Standard-Spaces der neuen Administrator-ID zu.
  - Die Berechtigung für Seiten und Spaces in Business Space können Sie in Business Space beim Erstellen von Seiten und Spaces definieren und verwalten.
  - Informationen dazu, wer Business Space-Administratoraktionen in der Business Space-Umgebung ausführen kann, finden Sie unter „Rolle des Superusers für Business Space zuordnen“ auf Seite 292.

**Anmerkung:**

Falls Sie die folgenden Fehler in der Datei `SystemOut.log` finden, haben Sie möglicherweise Zusatzattribute in Ihrer Benutzerregistry, die nicht verarbeitet werden können:

```
00000046 SystemErr R Caused by: com.ibm.websphere.wim.exception.WIMSystemException: CWWIM1013E
    The value of the property secretary is not valid for entity uid=xxx,c=us,ou=yyy,o=ibm.com.
00000046 SystemErr R at com.ibm.ws.wim.adapter.ldap.LdapAdapter.setPropertyValue
(LdapAdapter.java:3338)
```

Definieren Sie folgende Attribute in der Datei `ConfigServices.properties`, um die Zusatzattribute zu umgehen:

```
com.ibm.mashups.user.userProfile = LIMITED
com.ibm.mashups.user.groupProfile = LIMITED
```

Die Datei `ConfigServices.properties` befindet sich bei einem eigenständigen Server im Pfad `stammverzeichnis_des_profils\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties` und bei einem Cluster im Pfad `stammverzeichnis_des_deployment_manager-profils\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties`. Wenn die Datei `ConfigServices.properties` geändert wurde, führen Sie den Befehl **updatePropertyConfig** mithilfe des `wsadmin`-Scripting-Clients aus und befolgen Sie dazu die Anweisungen in Schritt 4.d.

#### Anmerkung:

Wenn Sie in einem Cluster die Java EE-Sicherheit aktiviert haben, sollten Sie in Erwägung ziehen, den Eintrag in der Serverrichtlinie, die auf die Business Space-Hilfeposition angewendet wird, zu begrenzen.

Die Richtlinie für die Business Space-Hilfeposition lautet:

```
grant codeBase "file:${was.install.root}/profiles/profilname/temp/
knotenname/-" {

    permission java.security.AllPermission;

};
```

Begrenzen Sie die Richtlinie, indem Sie sie wie folgt ändern:

```
grant codeBase "file:${was.install.root}/profiles/profilname/temp/
knotenname/servername/BspaceHelpEAR_knotenname_servername/BspaceHelp.war/-"
{

    permission java.security.AllPermission;

};
```

#### SSO und SSL für Business Space einrichten:

Bei Umgebungen, in denen sich Business Space und Ihr Produktserver in verschiedenen Zellen befinden, richten Sie die Konfiguration für Single Sign-on (SSO) und Secure Sockets Layer (SSL) manuell ein.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Aktivieren der Anwendungssicherheit und Verwaltungssicherheit. Vgl. „Sicherheit für Business Space aktivieren“ auf Seite 280.



- Überprüfen der Registrierung Ihrer Benutzer-ID in der Benutzerregistry Ihres Produkts.

**Tipp:** Falls Sie separate Zellen konfiguriert haben, müssen Sie sicherstellen, dass SSO-Aspekte berücksichtigt werden (dass LTPA-Schlüssel und gemeinsam genutzte Benutzernamen/Realmnamen synchron sind und dass Zertifikate importiert werden, falls dies erforderlich sein sollte). In einigen Fällen können sich bei IBM Business Process Manager mehrere Repositories im Realm befinden; dies kann zu einem Realmabweichungsfehler führen. Informationen finden Sie unter Realm in einer Konfiguration für eingebundene Repositories verwalten in der Dokumentation von WebSphere Application Server.

1. Wenn Business Space über Fernzugriff mit Ihrem Produkt verbunden ist und sich die Knoten, auf denen Business Space und Ihr Produkt ausgeführt werden, nicht in derselben Zelle befinden, müssen Sie manuelle Schritte zur Aktivierung von SSO (Single Sign-On) ausführen. Wenn Sie beispielsweise mehrere Produkte verwenden und sich die Server auf unterschiedlichen Knoten befinden, müssen Sie SSO manuell konfigurieren, damit diese Produkte mit dem Business Space-Server interagieren können. Führen Sie zum Aktivieren von SSO die folgenden Schritte aus:
  - a. Öffnen Sie in der Administrationskonsole des jeweiligen Servers die Seite 'Globale Sicherheit', indem Sie auf **Sicherheit > Globale Sicherheit** klicken. Erweitern Sie **Web- und SIP-Sicherheit** und klicken Sie unter 'Authentifizierung' auf **Single Sign-On (SSO)**, um sicherzustellen, dass das Kontrollkästchen **Aktiviert** ausgewählt ist.
  - b. Stellen Sie sicher, dass die Angaben unter **Benutzer-Repository** für alle Knoten identisch sind (siehe Schritt 3).
  - c. Führen Sie die Schritte aus, die unter Schlüssel importieren und exportieren im Information Center zu WebSphere Application Server beschrieben sind.
2. Wenn Sie HTTPS in der Endpunktdatei verwenden, sich die Endpunktposition auf einem anderen Knoten als Business Space befindet und das SSL-Zertifikat (SSL = Secure Sockets Layer) ein selbst signiertes SSL-Zertifikat ist, müssen Sie es importieren.

Stellen Sie sicher, dass die Unterzeichner in den entsprechenden Truststores für den Business Space-Server und den Produktserver konfiguriert sind. Weitere Informationen finden Sie unter Sichere Kommunikation mit Secure Sockets Layer (SSL) im Information Center zu WebSphere Application Server.

Weitere Informationen zu SSO und SSL finden Sie im Information Center für WebSphere Application Server.

### **HTTP- oder HTTPS-Einstellungen für Business Space einrichten:**

Standardmäßig ist Business Space für den Zugriff über HTTPS konfiguriert. Wenn Sie dies in HTTP ändern wollen, oder aus einer früheren Einstellung zu HTTPS zurückkehren wollen, verwenden Sie das Script `configBspaceTransport.py`.

Das Script `configBspaceTransport.py` befindet sich im Verzeichnis `installationsstammverzeichnis\BusinessSpace\scripts`. Ändern Sie die Datei `web.xml` mit dem Wert `allowhttp`, damit sowohl HTTP- als auch HTTPS-Verbindungen zugelassen werden. Mit dem Wert `httpsonly` wird die Datei `web.xml` so geändert, dass nur HTTPS-Verbindungen zugelassen werden, bzw. wird eine HTTP-Verbindung in HTTPS umgeleitet. Sie können das Script sowohl auf einem eigenständigen Server als auch im Deployment Manager einer Clusterumgebung ausführen.

1. Suchen Sie das Script *installationsstammverzeichnis*\BusinessSpace\scripts\configBspaceTransport.py zur Festlegung von HTTP- oder HTTPS-Einstellungen.
2. Öffnen Sie eine Eingabeaufforderung und wechseln Sie in das folgende Verzeichnis: *profilstammverzeichnis*\bin. Hierbei steht *profilstammverzeichnis* für das Verzeichnis des Profils, in dem Business Space installiert ist.
3. Führen Sie das Script configBspaceTransport.py mit einer der folgenden Optionen aus.
  - a. Damit HTTP-Verbindungen in Business Space zugelassen werden, geben Sie den folgenden Befehl ein: `wsadmin -lang jython -user benutzername -password kennwort -f configBspaceTransport.py -allowhttp` (damit sind sowohl HTTP- als auch HTTPS-Verbindungen zugelassen).
  - b. Damit nur HTTPS-Verbindungen in Business Space gestattet sind, geben Sie folgenden Befehl ein: `wsadmin -lang jython -user benutzername -password kennwort -f configBspaceTransport.py -httpsonly` (dies schaltet zur Standardkonfiguration zurück, die alle HTTP-Verbindungen in HTTPS umleitet).

Standardmäßig gilt der Befehl für den aktuellen Server- und Knotennamen bzw. den aktuellen Cluster, in dem der Befehl ausgeführt wird. Wenn Sie eine andere Arbeitsumgebung festlegen wollen, verwenden Sie die optionalen Parameter für den Server-/Knoten-/Clusternamen: `-serverName` und `-nodeName` oder `-clusterName`.

**Anmerkung:** Wenn der Pfad ein Leerzeichen enthält (*installationsstammverzeichnis* ist z. B. auf *mein installationsverzeichnis* gesetzt), müssen die Pfadnamen in Anführungszeichen gesetzt werden.

#### Sicherheit für System-REST-Services einrichten:

Um die Sicherheitsfunktion für die Daten in den Widgets auf der Basis von Benutzern und Gruppen einzurichten, müssen Sie die Zuordnung von Benutzern zur Gateway-Anwendung für REST-Services ändern.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Aktivieren der Anwendungssicherheit und Verwaltungssicherheit. Vgl. „Sicherheit für Business Space aktivieren“ auf Seite 280.
- Überprüfen der Registrierung Ihrer Benutzer-ID in der Benutzerregistry Ihres Produkts.

Die Zuordnung von Benutzern zu einer REST-Service-Provider-Anwendung wirkt sich auf alle Services des Providers aus.

Sie können die betroffenen Services anzeigen, indem Sie **Services > REST-Services > REST-Service-Provider** auswählen und dann die entsprechende Provider-Anwendung in der Liste auswählen.

1. Wählen Sie in der Administrationskonsole eine der folgenden Optionen aus:
  - Bei einer Serverumgebung: Wählen Sie **Anwendungen > Anwendungstypen > WebSphere-Enterprise-Anwendungen > REST-Service-Gateway** aus.
  - Zusätzlich bei einer Network Deployment-Umgebung: Wählen Sie **Anwendungen > Anwendungstypen > WebSphere-Enterprise-Anwendungen > REST-Service-Gateway-Dmgr** aus.
2. Wählen Sie im rechten Fenster unter 'Detaileigenschaften' die Option **Zuordnung von Sicherheitsrollen zu Benutzern/Gruppen** aus.

- Um den Zugriff auf Daten in den REST-Service-Widgets zu steuern, fügen Sie der Rolle **RestServicesUser** die entsprechenden Benutzer und Gruppen hinzu.

### **Sicherheitsaspekte bei Business Space-Widgets:**

Abhängig davon, welche Widgets Sie in Business Space mit Ihrem BPM-Produkt verwenden, können Sie den Zugriff auf Daten in einem Widget entweder durch die Zuordnung von Rollen zu Benutzergruppen mit Verwaltungsaufgaben oder durch die Zuordnung einer zusätzlichen Zugriffsebene auf Rollenbasis für das Widget steuern.

### **Verwaltungsgruppenrollen und Widgets**

Sie können den Zugriff auf Daten in Widgets über Verwaltungsgruppenrollen und die diesen Rollen zugeordneten Benutzer steuern. Sie können die diesen Rollen zugeordneten Benutzer anzeigen, indem Sie in der Administrationskonsole auf **Benutzer und Gruppen > Rollen für Gruppen mit Verwaltungsaufgaben** klicken und eine Gruppe auswählen. Die Liste der Rollen wird angezeigt.

Business-Regeln und Business-Variablen stellen zwei Beispiele für Widgets dar, deren Verwaltungsgruppenrollen möglicherweise geändert werden müssen.

Für das Widget 'Systemzustand' verfügen die folgenden Verwaltungsrollen über Überwachungsberechtigungen und erlauben den Zugriff auf die Administrationskonsole. Aus diesem Grund können Benutzer, denen diese Rollen zugeordnet sind, auf die Daten des Widgets 'Systemzustand' zugreifen:

- **Monitor**
- **Configurator**
- **Operator**
- **Administrator**
- **Adminsecuritymanager**
- **Deployer**
- **iscadmins**

Die Benutzer, die diesen Verwaltungsgruppenrollen zugeordnet sind, verfügen über Zugriff auf die Daten des Widgets 'Systemzustand'. Benutzer, die diesen Rollen nicht zugeordnet sind, können auf die Daten des Widgets 'Systemzustand' hingegen nicht zugreifen.

### **Rollenbasierter Zugriff auf Widgets**

#### **Tivoli Access Manager WebSEAL für Verwendung mit Business Space konfigurieren:**

Wenn Sie Tivoli Access Manager WebSEAL mit Business Space verwenden möchten, müssen Sie diverse zusätzliche Konfigurationsschritte ausführen.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Aktivieren der Anwendungssicherheit und Verwaltungssicherheit. Vgl. „Sicherheit für Business Space aktivieren“ auf Seite 280.
- Überprüfen der Registrierung Ihrer Benutzer-ID in der Benutzerregistry Ihres Produkts.
- Stellen Sie sicher, dass für Tivoli Access Manager und IBM Business Monitor dieselben Benutzer in den Benutzerregistries enthalten sind.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Monitor
- WebSphere Enterprise Service Bus
- IBM Business Process Manager

Wenn Sie Tivoli Access Manager WebSEAL mit Business Space verwenden möchten, müssen Sie WebSEAL für den kombinierten Einsatz mit Tivoli Access Manager konfigurieren, WebSEAL für den kombinierten Einsatz mit dem Anwendungsserver Ihres Produkts konfigurieren und Host-Junctions für Ihre Umgebung konfigurieren.

Wenn Sie IBM Business Process Manager haben und WebSEAL für den kombinierten Einsatz mit Process Portal in Ihrer IBM BPM-Umgebung konfigurieren, führen Sie Anweisungen im folgenden Abschnitt aus: Tivoli Access Manager WebSEAL zur Arbeit mit Process Portal konfigurieren.

1. Konfigurieren Sie WebSEAL für den kombinierten Einsatz mit Tivoli Access Manager.

- a. Stellen Sie sicher, dass WebSEAL ordnungsgemäß installiert und konfiguriert ist.
- b. Setzen Sie die folgenden Befehle ab, um einen Account für einen vertrauenswürdigen Benutzer in Tivoli Access Manager zu erstellen, der für die Konfiguration von TAI (Trust-Association-Interceptor) verwendet werden kann:

```
pdadmin -a sec_master -p domino123
```

```
pdadmin sec_master> user create -gsouser -no-password-policy taiuser  
"cn=taiuser,ou=websphere,o=ibm,c=us" taiuser taiuser ptaiuser
```

```
pdadmin sec_master> user modify taiuser password-valid yes
```

```
pdadmin sec_master> user modify taiuser account-valid yes
```

- c. Erstellen Sie die Junction zwischen WebSEAL und Ihrem Produktanwendungsserver mithilfe der Option **-c iv\_creds** für TAI++ und **-c iv\_user** für TAI. Geben Sie einen der folgenden Befehle in einer Zeile ein und verwenden Sie die für Ihre Umgebung zutreffenden Variablen:

Für TAI++

```
server task webseald-server create -t tcp -b supply -c iv_creds  
-h hostname -p websphere_app_portnummer /junction-name
```

**Tipp:** *junction-name* muss mit / beginnen.

- d. Definieren Sie die folgenden Parameter in der WebSEAL-Konfigurationsdatei *webseal\_installationsverzeichnis/etc/webseald-default.conf*:

```
basicauth-dummy-passwd=webseal_benutzer-id_kennwort
```

Beispiel: Wenn Sie die Benutzer taiuser/ptaiuser in Tivoli Access Manager festlegen, legen Sie den folgenden Parameter fest: basicauth-dummy-passwd = ptaiuser

Definieren Sie die folgenden Parameter, wenn Sie eine formularbasierte Authentifizierung verwenden:

```
forms-auth=both
```

```
ba-auth=none
```

2. Falls erforderlich, konfigurieren Sie WebSEAL für den kombinierten Einsatz mit Ihrem Produktanwendungsserver, indem Sie den Interceptor von TAI++ auf dem Server aktivieren.

- a. Wählen Sie in der Administrationskonsole **Globale Sicherheit > Authentifizierungsverfahren und Verfallszeit** aus.
- b. Erweitern Sie **Web- und SIP-Sicherheit** und wählen Sie anschließend **Trust Association** aus. Wählen Sie das Kontrollkästchen aus und klicken Sie auf **Anwenden**.
- c. Damit **TAMTrustAssociationInterceptorPlus** unter **Interceptor** angezeigt wird, fügen Sie `com.ibm.ws.security.web.TAMTrustAssociationInterceptorPlus` hinzu und starten den Server erneut.
- d. Wählen Sie **Interceptor > TAMTrustAssociationInterceptorPlus > Angepasste Eigenschaften** aus und fügen Sie die folgenden Eigenschaften hinzu:

Name	Wert
<code>com.ibm.websphere.security.webseal.configURL</code>	<code>\${WAS_INSTALL_ROOT}/java/jre/PdPerm.properties</code>
<code>com.ibm.websphere.security.webseal.id</code>	<code>iv-creds</code>
<code>com.ibm.websphere.security.webseal.loginId</code>	<code>taiuser</code> (falls der Benutzer <code>taiuser/ptaiuser</code> in Tivoli Access Manager erstellt wurde)

- e. Starten Sie die Zelle erneut.
  - f. Wechseln Sie zu `https://webseal_servername:webseal_port/junction name/web_uri_für_client`, um auf den Client zuzugreifen.
3. Konfigurieren Sie die Host-Junctions für Ihre Umgebung, sodass die Business Space-Widgets angezeigt werden. Verwenden Sie virtuelle Host-Junctions.
    - a. Stellen Sie sicher, dass ein virtueller Host konfiguriert worden ist. Virtuelle Host-Junctions stimmen mit einem Host und einer Portnummer überein und leiten Adressen an den Zielhost weiter. Es findet keine URL-Filterung statt, und alle Anforderungen, die übereinstimmen, werden an den Zielhost weitergeleitet.
    - b. Stellen Sie sicher, dass die folgenden Anwendungen dem virtuellen Host zur Verfügung stehen. Sie verfügen möglicherweise über alle oder nur einige der Anwendungen, je nachdem, welche Produkte Sie mit Business Space verwenden.
      - `BPMAAdministrationWidgets_knotenname_servername` (für WebSphere Enterprise Service Bus und IBM Business Process Manager)
      - `BusinessSpaceHelpEAR_knotenname_servername` (für alle Produkte)
      - `BSpaceEAR_knotenname_servername` (für alle Produkte)
      - `BSpaceForms_knotenname_servername` (für alle Produkte)
      - `HumanTaskManagementWidgets_knotenname_servername` (für IBM Business Process Manager und IBM Business Monitor)
      - `PageBuilder2_knotenname_servername` (für alle Produkte)
      - `REST Services Gateway` (für alle Produkte)
      - `REST Services Gateway Dmgr` (für WebSphere Enterprise Service Bus und IBM Business Process Manager)
      - `mm.was_knotenname_servername` (für alle Produkte)
      - `WBMDashboardWeb_knotenname_servername` (für IBM Business Monitor)
      - `webWidgets_knotenname_servername` (für WebSphere Enterprise Service Bus)

**Anmerkung:** Diese Liste der Anwendungen umfasst lediglich die für Business Space erforderlichen Anwendungen. Möglicherweise müssen Sie weite-

re Anwendungen in die Liste für Szenarios ohne Business Space mit Tivoli Access Manager WebSEAL mitaufnehmen.

- c. Führen Sie den folgenden Befehl mithilfe von `pdadmin` aus: `server task webseal server virtualhost create -t transport -h zielhost [-p port] [-v name_des_virtuellen_hosts] bezeichnung_des_virtuellen_hosts`

Verwenden Sie die folgenden Informationen:

- `webseal server` ist der Name des WebSEAL-Servers, auf dem Sie den Eintrag für den virtuellen Host erstellen.
- `transport` ist der Transporttyp. Gültige Einträge sind `tcp`, `ssl`, `tcpproxy`, und `sslproxy`.
- `zielhost` ist der Host der erforderlichen Anwendung.
- `name_des_virtuellen_hosts` wird verwendet, um HTTP-Anforderungen mit einer virtuellen Host-Junction abzugleichen. Wird kein Wert eingegeben, wird er standardmäßig aus Zielhost und Port zusammen gesetzt. Beispiel: Wenn Sie `name_des_virtuellen_hosts` auf `myvirthost.ibm.com:80` setzen, gleicht WebSEAL die URLs ab, die `myvirthost.ibm.com:80` enthalten und leitet sie an den Host, der im Befehl 'pdadmin' angegeben wurde.
- `bezeichnung_des_virtuellen_hosts` ist die Bezeichnung, unter der der Eintrag in WebSEAL identifiziert wird. Sie muss eindeutig sein.

Damit Business Space ordnungsgemäß ausgeführt werden kann, müssen als Transporttyp die beiden Einträge `ssl` und `tcp` erstellt werden. Wenn es für Sie erforderlich ist, dass sowohl SSL (Secure Sockets Layer) als auch TCP (Transmission Control Protocol) in derselben virtuellen Host-Junction unterstützt werden, müssen Sie die Option `-g`

`bezeichnung_des_virtuellen_hosts` verwenden; dabei gilt, dass `bezeichnung_des_virtuellen_hosts` die Bezeichnung des ursprünglichen virtuellen Hosts ist, dessen Konfiguration gemeinsam genutzt werden soll. Mit dieser Option wird nach einer früher erstellten virtuellen Host-Junction gesucht (die zuvor erstellt wurde und in der die `bezeichnung_des_virtuellen_hosts` mit der Bezeichnung in der Option `-g` übereinstimmt) und die entsprechende Konfiguration gemeinsam genutzt. Der zweite Eintrag erfordert zwar eine eigene `bezeichnung_des_virtuellen_hosts`, kann jedoch den Zielhost, den Port und andere Werte gemeinsam nutzen. Wenn Sie die Option `-g` nicht angeben, kann kein zweiter virtueller Host erstellt werden, da für WebSEAL der Zielhost und der Port identisch mit einer zuvor erstellten Junction sind (was nicht zulässig ist).

4. Führen Sie zusätzliche Konfigurationsschritte aus, um Probleme mit Browser-Cookies und virtuellen Hosts zu lösen.
- a. Nehmen Sie zwecks Umbenennung des Business Space-Cookies den folgenden Inhalt in die WebSEAL-Konfigurationsdatei auf:
- ```
[preserve-cookie-names]
name = com.ibm.bspace.UserName
name = com.ibm.wbimonitor.UserName
```
- b. Optional: Wenn Sie keine standardmäßigen virtuellen Hosts für einen Stammkontext verwenden, treten möglicherweise Probleme in den Business Space-Seiten auf. Eventuell müssen Sie das Umschreiben des JavaScript durch die Junction auf den Business Space-Seiten stoppen, indem Sie die Junction `-j` dem Stammkontext hinzufügen. Führen Sie den folgenden Befehl aus: `server task default-webseald create -f -h hostname -p portnummer -t tcp -b supply -c iv-user,iv-creds,iv-groups -x -s -j -J trailer/stammkontext`

**Rolle des Superusers für Business Space zuordnen:**



In Business Space können Sie Benutzern die Rolle des Superusers (oder Business Space-Administrators) zuordnen. Ein Superuser kann alle Speicherbereiche und Seiten anzeigen, bearbeiten und löschen, Vorlagen verwalten und erstellen sowie das Eigentumsrecht an einem Speicherbereich durch Ändern der Eigner-ID ändern.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Aktivieren der Anwendungssicherheit und Verwaltungssicherheit. Vgl. „Sicherheit für Business Space aktivieren“ auf Seite 280.
- Überprüfen der Registrierung Ihrer Benutzer-ID in der Benutzerregistry Ihres Produkts.

Ordnen Sie die Rolle des Business Space-Superusers zu und verwenden Sie dazu die folgende Rolle für die Anwendungsserversicherheit: **Admin**. Dieses Verfahren bietet Ihnen die Flexibilität, die Rolle einer beliebigen Zahl von Gruppen und Benutzern in Ihrem Unternehmen zuzuordnen. Dabei ist es nicht erforderlich, in der Benutzerregistry eine Administratorgruppe zu erstellen, die ausschließlich als Focal Point für den Business Space-Superuser dient.

Wenn der Business Space-Superuser bereits in einer Version vor V7.5 zugeordnet wurde, können Sie den Superuser stattdessen nach Benutzergruppe ändern. Weitere Informationen finden Sie unter Business Space-Superuser nach Benutzergruppe zuordnen.

- Wenn Sie die Business Space-Administratoren zum ersten Mal mit der Superuser-Rolle einrichten, führen Sie die folgenden Schritte aus:
  1. Melden Sie sich an der Administrationskonsole Ihres Produkts an.
  2. Klicken Sie auf **Anwendungen > Anwendungstypen > WebSphere-Enterprise-Anwendungen** und wählen Sie eine der folgenden Anwendungen aus:
    - **mm.was\_knoten\_server** (für eine eigenständige Serverumgebung)
    - **mm.was\_cluster** (für eine Network Deployment-Umgebung)
  3. Klicken Sie auf **Sicherheitsrolle zu Benutzern/Gruppen zuordnen**.
  4. Wählen Sie die Zeile für die Rolle **Admin** aus und klicken Sie auf die Schaltfläche **Benutzer zuordnen** oder auf die Schaltfläche **Gruppen zuordnen**, um entweder Benutzer oder Gruppen der Rolle 'Admin' zuzuordnen.
  5. Klicken Sie auf **Speichern**.
  6. Starten Sie den Server erneut.
- Wenn Sie Superuser zuvor auf der Basis von Benutzergruppen zugeordnet haben und Sie stattdessen ein einfacheres Verfahren anwenden möchten, bei dem die Superuser nach Rolle verwaltet werden, führen Sie folgende Schritte aus:
  1. Öffnen Sie die Konfigurationsdatei.
    - Eigenständiger Server: `profilstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties`
    - Cluster: `deployment_manager-profilstammverzeichnis\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties`
  2. Ändern Sie die folgenden Eigenschaftswerte in der Konfigurationsdatei.  
`com.ibm.mashups.adminGroupName = {com.ibm.mashups.J2EERole.Admin}`  
`com.ibm.mashups.widget.attributes.configure.groups=`
  3. Führen Sie den Befehl **updatePropertyConfig** in der wsadmin-Umgebung des Profils aus.

**Wichtig:** Für Windows muss der Wert für den Parameter **propertyFileName** der vollständige Pfad zu der Datei sein, und alle Backslashes müssen doppelt angegeben werden. Beispiel: `AdminTask.updatePropertyConfig('[-serverName servername -nodeName knotenname -propertyFileName "profilstammverzeichnis\\BusinessSpace\\knotenname\\servername\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')`.

– Eigenständiger Server:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-serverName servername -nodeName knotenname
-propertyFileName "profilstammverzeichnis\\BusinessSpace\\knotenname\\servername
\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')
```

`AdminConfig.save()`

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-serverName servername -nodeName knotenname
-propertyFileName "profilstammverzeichnis\\BusinessSpace\\knotenname\\servername
\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

– Cluster:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-clusterName clustername -propertyFileName
"deployment_manager-profilstammverzeichnis\\BusinessSpace\\clustername\\mm.runtime.prof\\
config\\ConfigService.properties" -prefix "Mashups_"]')
```

`AdminConfig.save()`

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-clusterName clustername -propertyFileName
"deployment_manager-profilstammverzeichnis\\BusinessSpace\\clustername\\mm.runtime.prof\\
config\\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

4. Starten Sie den Server erneut.
5. Führen Sie den vorherigen Schritt aus, um Benutzern Business Space-Superuser-Rollen zuzuordnen.

### Business Space-Superuser nach Benutzergruppe zuordnen:

Sie können Business Space-Benutzer auf der Basis von Benutzergruppen als Superuser (oder Business Space-Administratoren) zuordnen.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Aktivieren der Anwendungssicherheit und Verwaltungssicherheit. Vgl. „Sicherheit für Business Space aktivieren“ auf Seite 280.
- Überprüfen der Registrierung Ihrer Benutzer-ID in der Benutzerregistry Ihres Produkts.

**Tipp:** Wenn Sie zuvor Benutzergruppen verwendet haben, um die Business Space-Superuser-Rolle zuzuordnen, können Sie nun das einfachere Verfahren zur Zuordnung von Business Space-Superusers nach Rolle nutzen. Vgl. „Rolle des Superusers für Business Space zuordnen“ auf Seite 292.

Ein Superuser kann alle Speicherbereiche und Seiten anzeigen, bearbeiten und löschen, Schablonen verwalten und erstellen sowie das Eigentumsrecht an einem Speicherbereich durch Ändern der Eigner-ID ändern.

Falls die Verwaltungssicherheit aktiviert ist, während Sie Business Space konfigurieren, sollten Sie die folgenden Informationen über Gruppen und Superuser berücksichtigen:

- Benutzer, die zu der besonderen Benutzergruppe **Administratoren** gehören, verfügen standardmäßig über die Superuser-Rolle. Daher erfolgt die Zuordnung der Rolle 'Superuser' durch die Benutzergruppenzugehörigkeit.
- In einer Einzelserverumgebung erstellt der Business Space-Server die Benutzergruppe **Administratoren** in der standardmäßigen Benutzerregistry. Die bei der Konfiguration bereitgestellte Administrator-ID wird automatisch als Mitglied zu dieser Gruppe hinzugefügt.
- In einer Network Deployment-Umgebung wird die Benutzergruppe **Administratoren** nicht automatisch erstellt. Verwenden Sie das Script `createSuperUser.py`, um die Benutzergruppe zu erstellen und in der standardmäßigen Benutzerregistry Mitglieder zu dieser Gruppe hinzuzufügen.
- Wenn anstelle der standardmäßigen Benutzerregistry eine andere Benutzerregistry (beispielsweise LDAP) verwendet wird, oder falls die standardmäßige Benutzerregistry verwendet wird, Sie jedoch nicht die Benutzergruppe **Administratoren** verwenden möchten, müssen Sie die Benutzergruppe angeben, die Sie für die Business Space-Superusers verwenden. Stellen Sie sicher, dass der Wert, den Sie angeben, von der Benutzerregistry verstanden werden kann. Für LDAP können Sie z. B. einen Namen wie `cn=administrators,dc=company,dc=com` angeben. Weitere Informationen zur Angabe dieser Benutzergruppe finden Sie in den Anleitungen zum Ändern von Administratorgruppen im Abschnitt mit den weiteren Schritten.
- Bei Business Space in WebSphere Portal wird auch die Standardgruppe **wpsadmins** für die Rolle 'Superuser' verwendet. Mitgliedern dieser Gruppe wird die Rolle 'Superuser' für Business Space erteilt.

**Anmerkung:** Die Sicherheit muss aktiviert sein, um Business Space in WebSphere Portal verwenden zu können.

Wenn die Verwaltungssicherheit nicht aktiviert ist wenn Sie Business Space konfigurieren, hat nur die spezielle Benutzer-ID **BPMAdministrator** die Rolle des Business Space-Superusers.

In einer Network Deployment-Umgebung müssen Sie das Script `createSuperUser.py` ausführen, um die Rolle Superuser' zuzuordnen: zum Erstellen der Benutzergruppe und zum Hinzufügen von Mitgliedern. Führen Sie vor der Ausführung des Scripts die folgenden Schritte aus:

- Stellen Sie sicher, dass der Standardname der Gruppe **Administratoren** nicht geändert wird.
  - Verwenden Sie das Standard-Repository für die Benutzerregistry.
  - Starten Sie den Server oder Deployment Manager der Business Space-Umgebung für das Profil, in dem Business Space installiert ist.
1. Suchen Sie das Script `installationsstammverzeichnis\BusinessSpace\scripts\createSuperUser.py`, um einem Benutzer die Rolle des Superusers zuzuordnen.
  2. Öffnen Sie eine Eingabeaufforderung und wechseln Sie in das folgende Verzeichnis: `profilstammverzeichnis\bin`. Hierbei steht `profilstammverzeichnis` für das Verzeichnis des Profils, in dem Business Space installiert ist.
  3. Geben Sie den folgenden Befehl ein: `wsadmin -lang jython -f installationsstammverzeichnis\BusinessSpace\scripts\createSuperUser.py benutzerkurzname kennwort` Dabei ist `benutzerkurzname` die eindeutige Kennung für einen Benutzer in VMM (Virtual Member Manager) und `kennwort` das

VMM-Kennwort für diesen Benutzer. Wenn dieser Benutzer in VMM vorhanden ist, wird er zur Administratorgruppe hinzugefügt.

**Anmerkung:** Wenn der Pfad ein Leerzeichen enthält (*installationsstammverzeichnis* ist z. B. auf mein installationsverzeichnis gesetzt), müssen die Pfadnamen in Anführungszeichen gesetzt werden. Geben Sie beispielsweise den folgenden Befehl ein: `wsadmin -lang jython -f "\mein installationsverzeichnis\BusinessSpace\scripts\createSuperUser.py" be-  
nutzerkurzname_in_VMM`.

Um Business Space zu öffnen, geben Sie die folgende URL ein: `http://host:port/BusinessSpace`. Hierbei steht *host* für den Namen des Hosts, auf dem Ihr Server ausgeführt wird, und *port* steht für die Portnummer Ihres Servers.

Sie können die standardmäßige spezielle Benutzergruppe **Administratoren** ändern. Führen Sie folgende Schritte aus, um den aktuellen Gruppennamen zu prüfen oder zu ändern.

Überprüfen Sie den Wert für den Messwert `com.ibm.mashups.adminGroupName` in der Konfigurationsdatei:

- `installationsstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties` auf einem eigenständigen Server
- `stammverzeichnis_des_deployment_manager-profil\BusinessSpace\clusternamen\mm.runtime.prof\config\ConfigService.properties` in einem Cluster

**Wichtig:** Für Windows muss beim Ausführen des Befehls **updatePropertyConfig** der Wert für den Parameter **propertyFileName** der vollständige Pfad zu der Datei sein, und alle Backslashes müssen doppelt angegeben werden. Beispiel:

```
AdminTask.updatePropertyConfig('[-serverName servername -nodeName  
knotenname -propertyFileName "profilstammverzeichnis\BusinessSpace\  
knotenname\servername\mm.runtime.prof\config\ConfigService.properties"  
-prefix "Mashups_"]')
```

Wenn Sie eine Verwaltungsgruppe ändern wollen, müssen Sie auf einem eigenständigen Server folgende Schritte ausführen:

1. Stellen Sie sicher, dass die Gruppe im Benutzerrepository vorhanden ist.
2. Ändern Sie den Messwert `com.ibm.mashups.adminGroupName` in der Konfigurationsdatei `installationsstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties`.
3. Führen Sie den Befehl 'updatePropertyConfig' in der wsadmin-Umgebung des Profils: `$AdminTask updatePropertyConfig {-serverName servername -nodeName knotenname -propertyFileName "stammverzeichnis_des_profil\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} und anschließend $AdminConfig save aus.`
4. Starten Sie den Server erneut.

Wenn Sie eine Verwaltungsgruppe ändern wollen, müssen Sie in einem Cluster folgende Schritte ausführen:

1. Stellen Sie sicher, dass die Gruppe im Benutzerrepository vorhanden ist.

2. Ändern Sie den Messwert `com.ibm.mashups.adminGroupName` in der Konfigurationsdatei `stammverzeichnis_des_deployment_manager-profils\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties`.
3. Führen Sie den Befehl 'updatePropertyConfig' in der wsadmin-Umgebung des Implementierungsumgebungsprofils: `$AdminTask updatePropertyConfig {-clusterName clustername -propertyFileName "stammverzeichnis_des_deployment_manager-profils\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}` und anschließend `$AdminConfig save aus`.
4. Führen Sie einen Neustart des Deployment Managers aus.

Wenn Sie bei nicht aktivierter Sicherheit den Superuser ändern wollen, müssen Sie auf einem eigenständigen Server folgende Schritte ausführen:

1. Ändern Sie den Messwert `noSecurityAdminInternalUserOnly` in der Konfigurationsdatei `installationsstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties`.
2. Führen Sie den Befehl 'updatePropertyConfig' in der wsadmin-Umgebung des Profils: `$AdminTask updatePropertyConfig {-serverName servername -nodeName knotenname -propertyFileName "stammverzeichnis_des_profils\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}` und anschließend `$AdminConfig save aus`.
3. Starten Sie den Server erneut.

Wenn Sie bei nicht aktivierter Sicherheit den Superuser ändern wollen, müssen Sie in einem Cluster folgende Schritte ausführen:

1. Ändern Sie den Messwert `noSecurityAdminInternalUserOnly` in der Konfigurationsdatei `stammverzeichnis_des_deployment_manager-profils\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties`.
2. Führen Sie den Befehl 'updatePropertyConfig' in der wsadmin-Umgebung des Implementierungsumgebungsprofils: `$AdminTask updatePropertyConfig {-clusterName clustername -propertyFileName "stammverzeichnis_des_deployment_manager-profils\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}` und anschließend `$AdminConfig save aus`.
3. Führen Sie einen Neustart des Deployment Managers aus.

### **Berechtigung zum Erstellen von Business Spaces auf bestimmte Benutzer einschränken:**

Sie können Business Space anpassen, sodass nur Benutzer, die sich mit einer Superuser-Rolle anmelden, Business Spaces erstellen können.

Standardmäßig können alle Benutzer Business Spaces erstellen. Sie können jedoch Business Space sperren, sodass lediglich Benutzer, die sich mit einer Superuser-ID anmelden, Business Spaces erstellen oder importieren können.

**Wichtig:** Die Sperrprozedur, die in diesem Abschnitt beschrieben wird, gilt nur für die Business Space-Benutzerschnittstelle. Sie schränkt den sonstigen Zugriff auf Business Space nicht ein.

Diese Superuser (oder Business Space-Administratoren) können einen Business Space erstellen und das Eigentumsrecht auf andere Benutzer übertragen. Die Benutzer, denen das Eigentumsrecht zugeordnet wurde, können die Spaces dann so

verwalten, als hätten sie sie selbst erstellt. Beispielsweise können sie festlegen, wer den Space und seine Eigenschaften anzeigen und bearbeiten kann, und sie können Seiten hinzufügen.

**Anmerkung:** Die Möglichkeit, Benutzer daran zu hindern, Business Spaces zu erstellen, ist für Business Space auf WebSphere Portal Server nicht verfügbar.

Führen Sie die folgenden Schritte aus, wenn Sie festlegen wollen, dass nur Superuser berechtigt sind, Business Spaces zu erstellen.

1. Ändern Sie in der folgenden Konfigurationsdatei den Wert für die Einstellung `com.ibm.mashups.lockeddown` in `true`:
  - Eigenständiger Server: `profilstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties`
  - Cluster: `deployment_manager-profilstammverzeichnis\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties`

Der Standardwert `false` bedeutet, dass alle Benutzer Business Spaces erstellen können. Wenn der Wert auf `true` gesetzt ist, können lediglich Superuser Business Spaces erstellen.

2. Führen Sie den Befehl **updatePropertyConfig** in der `wsadmin`-Umgebung des Profils aus:

- Eigenständiger Server:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig(['-serverName servername -nodeName knotenname  
-propertyFileName "profilstammverzeichnis\BusinessSpace\knotenname\servername  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"'])  
AdminConfig.save()
```

**Wichtig:** Für Windows muss der Wert für den Parameter **propertyFileName** der vollständige Pfad zu der Datei sein, und alle Backslashes müssen doppelt angegeben werden. Beispiel: `AdminTask.updatePropertyConfig(['-serverName servername -nodeName knotenname -propertyFileName "profilstammverzeichnis\\BusinessSpace\\knotenname\\servername\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"'])`.

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-serverName servername -nodeName knotenname  
-propertyFileName "profilstammverzeichnis\BusinessSpace\knotenname\servername  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

- Cluster:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig(['-clusterName clustername -propertyFileName  
"deployment_manager-profilstammverzeichnis\BusinessSpace\clustername\mm.runtime.prof\  
config\ConfigService.properties" -prefix "Mashups_"'])  
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-clusterName clustername -propertyFileName  
"deployment_manager-profilstammverzeichnis\BusinessSpace\clustername\mm.runtime.prof\  
config\ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

Wenn sich Benutzer das nächste Mal bei Business Space anmelden, sind sie nicht in der Lage, einen Business Space zu erstellen, es sei denn, sie melden sich mit einer Superuser-ID an.



## Suchvorgänge für Benutzerregistries ohne Platzhalter aktivieren:

Wenn Ihre Benutzerregistry so eingerichtet ist, dass keine Platzhalter verwendet werden, müssen Sie zusätzliche Konfigurationsschritte ausführen, damit Suchvorgänge in Business Space richtig ausgeführt werden. Dies gilt auch für Widgets, die die Benutzerregistry durchsuchen.

Vor der Ausführung dieser Task müssen Sie die folgenden Tasks ausführen:

- Aktivieren der Anwendungssicherheit und Verwaltungssicherheit. Vgl. „Sicherheit für Business Space aktivieren“ auf Seite 280.
- Überprüfen der Registrierung Ihrer Benutzer-ID in der Benutzerregistry Ihres Produkts.

Wenn ein Business Space-Benutzer durch Eingabe von ein oder mehr Zeichen nach Benutzern oder Gruppen sucht, fügt Business Space automatisch Platzhalterzeichen hinzu. Dies ist die Standardeinstellung. Beispiel: Wenn die Benutzerregistry ein LDAP-Server ist und der Benutzer `smit` eingibt, konvertiert Business Space dies in eine Abfrage `*smit*`, sodass als Suchergebnis Namen wie z. B. `Smith`, `Smithers` und `Psmith` zurückgegeben werden. Wenn Sie die automatischen Platzhalter aber nicht verwenden wollen - z. B. weil Ihre Benutzerregistry dies nicht zulässt - können Sie diese Funktionalität inaktivieren.

Um die automatische Platzhaltersuche für Ihre Umgebung zu inaktivieren, führen Sie folgende Schritte aus:

- Bei einem eigenständigen Server führen Sie folgende Schritte aus:
  1. Aktualisieren Sie die Konfigurationsdatei `profilstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties` mit `com.ibm.mashups.user.stripWildcards=true`.
  2. Führen Sie den Befehl **updatePropertyConfig** in der 'wsadmin'-Umgebung des Profils aus:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-serverName servername -nodeName knotenname -propertyFileName "profile_root\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
```

```
AdminConfig.save()
```

**Wichtig:** Für Windows muss der Wert für den Parameter **propertyFileName** der vollständige Pfad zu der Datei sein, und alle Backslashes müssen doppelt angegeben werden. Beispiel: `AdminTask.updatePropertyConfig('[-serverName servername -nodeName knotenname -propertyFileName "profilstammverzeichnis\\BusinessSpace\\knotenname\\servername\\mm.runtime.prof\\config\\ConfigService.properties" -prefix "Mashups_"]')`.

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-serverName servername -nodeName knotenname -propertyFileName "profilstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
```

```
$AdminConfig save
```

3. Starten Sie den Server erneut.
- Bei einem Cluster führen Sie folgende Schritte aus:

1. Aktualisieren Sie die Konfigurationsdatei `stammverzeichnis_deployment_manager-profil\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties` mit `com.ibm.mashups.user.stripWildcards=true`.
2. Führen Sie vom Deployment Manager aus den Befehl `updatePropertyConfig` in der wsadmin-Umgebung des Profils aus:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-clusterName clustername
-propertyFileName "deployment_manager-profilstammverzeichnis\
BusinessSpace\clustername\mm.runtime.prof\config\
ConfigService.properties" -prefix "Mashups_"]')
```

AdminConfig.save()

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-clusterName clustername
-propertyFileName "deployment_manager-profilstammverzeichnis\
BusinessSpace\clustername\mm.runtime.prof\config\
ConfigService.properties" -prefix "Mashups_"}
```

\$AdminConfig save

3. Führen Sie einen Neustart des Deployment Managers aus.

## Befehle ('wsadmin'-Scripting) zum Konfigurieren von Business Space

Suchen Sie nach einem Scripting-Objekt oder einer Befehlsklasse, um Details zur zugehörigen Befehlssyntax zu finden.

Das Tool `wsadmin` befindet sich unter `<WAS_INSTALL_DIR>/bin` und `<WAS_PROFILE_DIR>/bin`. Verwenden Sie einen der folgenden Befehle, um es zu starten:

- Mit Jython:

```
> Windows wsadmin -lang jython
> Linux UNIX ./wsadmin.sh -lang jython
```

- Mit Jacl:

```
> Windows wsadmin
> Linux UNIX ./wsadmin.sh
```

Für die meisten Business Space-Befehle wird empfohlen, das Tool `wsadmin` im nicht verbundenen Modus (d. h. mit gestopptem Server) auszuführen. Zu diesem Zweck verwenden Sie den Parameter `-conntype NONE`:

- Mit Jython:

```
> Windows wsadmin -lang jython -conntype NONE
> Linux UNIX ./wsadmin.sh -lang jython -conntype NONE
```

- Mit Jacl:

```
> Windows wsadmin -conntype NONE
> Linux UNIX ./wsadmin.sh -conntype NONE
```

Zum Öffnen des Inhaltsverzeichnisses des Information Center an der Position dieser Referenzinformationen klicken Sie auf die Schaltfläche **In Inhaltsverzeichnis anzeigen** am Rand Ihres Information Center.

## Befehl **addICMSystem**:

Verwenden Sie den Befehl **addICMSystem** um Endpunkte für IBM Case Manager-Services zur Endpunktregistrierungsdatei für IBM BPM hinzuzufügen. Damit kann die eingebundene REST API auf dem IBM BPM Advanced-Server mit dem IBM Case Manager -Server eine Verbindung aufbauen.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

Dieser Befehl muss dort ausgeführt werden, wo die IBM BPM eingebundene REST API implementiert ist. Geben Sie bei der Ausführung dieses Befehls auch die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

### Erforderliche Parameter

**-icmCellName** *zellename*

Ein Parameter, der den Namen der IBM Case Manager-Zelle angibt.

**-icmNodeName** *knotenname*

Ein Parameter, der den Namen des IBM Case Manager-Knoten für die Konfiguration angibt. Wenn Sie den Parameter **icmClusterName** nicht angeben, müssen Sie die beiden Parameter **icmServerName** und **icmNodeName** setzen.

**-icmServerName** *servername*

Ein Parameter, der den Namen des IBM Case Manager-Servers für die Konfiguration angibt. Wenn Sie den Parameter **icmClusterName** nicht angeben, müssen Sie die beiden Parameter **icmServerName** und **icmNodeName** setzen.

**-icmClusterName** *clustername*

Ein Parameter, der den Namen des IBM Case Manager-Clusters für die Konfiguration angibt. Zur Konfiguration von Business Space auf einem Cluster müssen Sie den Parameter **icmClusterName** ohne die Parameter **icmServerName** und **icmNodeName** angeben.

**-PEConnectionName** *verbindungsname*

Ein Parameter, der den Verbindungsnamen für die Prozessengine von IBM Case Manager angibt.

**-icmHostName** *hostname*

Ein Parameter, der den Namen des IBM Case Manager-Hosts angibt.

**-icmPort** *port*

Ein Parameter, der die Portnummer des IBM Case Manager-Hosts angibt.

**-icmTransportType** *http | https*

Ein Parameter, der angibt, ob die eingebundene REST API das HTTP- oder das HTTPS-Protokoll verwendet.

### Optionale Parameter

**-federateSystem** *true | false*

Wenn dieser Parameter auf `true` (wahr) gesetzt wird, wenn die Einbindungsdomäne namens `BPM_ICM_Federation_Domain` nicht existiert, wird er mit zwei Systemen - ICM und BPM - erstellt. Standardmäßig ist `false` (falsch) gesetzt; dies bedeutet, es wird keine Domäne erstellt oder verändert. Sie können die Domäne auch mithilfe der vorhandenen Befehle zur Einbindung von Domänen, beispielsweise **modifyBPMApiFederationDomain** verwenden.

## Beispiel

Die folgenden Beispiele verwenden den Befehl **addICMSystem**, um HTTPS-Endpunkte für IBM Case Manager-Services in IBM BPM hinzuzufügen, ohne IBM Case Manager zu einer eingebundenen Domäne hinzuzufügen.

Beispiel mit Jython:

```
AdminTask.addICMSystem(['-icmCellName zellename  
-icmClusterName clustername  
-PEConnectionName verbindungsname  
-icmHostName hostname  
-icmPort port  
-icmTransportType https  
-federateSystem false']')
```

Beispiel mit Jacl:

```
$AdminTask addICMSystem {-icmCellName zellename  
-icmClusterName clustername  
-PEConnectionName verbindungsname  
-icmHostName hostname  
-icmPort port  
-icmTransportType https  
-federateSystem false}
```

## Befehl 'configureBusinessSpace':

Verwenden Sie den Befehl **configureBusinessSpace**, um die Datenbank für Business Space powered by WebSphere zu konfigurieren.

Mit diesem Befehl wird die Datenquelle für Business Space konfiguriert und die Scripts zum Erstellen und Konfigurieren der Datenbanktabellen generiert.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:  
AdminConfig.save()
- Jacl:  
\$AdminConfig save

Geben Sie die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

## Erforderliche Parameter

### **-serverName** *servername*

Dieser Parameter gibt den Servernamen für die Konfiguration an. Für die Konfiguration von Business Space auf einem Server muss ein **Servername** und ein **Knotenname** angegeben werden.

### **-nodeName** *knotenname*

Dieser Parameter gibt den Knotennamen für die Konfiguration an. Für die Konfiguration von Business Space auf einem Server muss ein **Servername** und ein **Knotenname** angegeben werden.

### **-clusterName** *clustername*

Dieser Parameter gibt den Clusternamen für die Konfiguration an. Für die Konfiguration von Business Space in einem Cluster muss ein **Clustername** angegeben werden.

## Optionale Parameter

### **-createTables true|false**

Gibt an, ob Sie die Business Space-Datenbanktabellen erstellen möchten. Wenn der Wert `true` gesetzt ist, wird die Datenbank für DB2, Oracle, oder SQL Server mit Business Space-Tabellen konfiguriert. Die Angabe des Parameters `true` setzt voraus, dass die Business Space-Datenbank bereits erstellt wurde, bevor dieser Befehl ausgeführt wird. Der Standardwert lautet `false`.

### **-dbName datenbankname**

Gibt die Datenbank an, die Sie für Business Space verwenden. Wenn Ihr Anwendungsserver und DB2 sich auf demselben z/OS-Image befinden, müssen Sie den Parameter **-dbName** angeben.

### **-dbWinAuth true|false**

Gibt an, ob Sie Windows-Authentifizierung mit Microsoft SQL Server verwenden. Wenn Sie die Windows-Authentifizierung in Ihrer SQL-Serverumgebung verwenden möchten, müssen Sie den Parameter auf `true` setzen. Der Standardwert ist `false`.

### **-schemaName schemaname**

Ein optionaler Parameter, der das Datenbankschema für die Datenbankkonfiguration von Business Space angibt. Der Standardwert lautet `IBMBUSSP`.

### **-tablespaceDir tabellenbereichspfad**

Ein optionaler Parameter, der einen Verzeichnispfad oder ein Dateinamenpräfix für die Dateien angibt, die als physische Positionen von Tabellenbereichen verwendet werden. Der Standardwert lautet `BSP`. Gültig für DB2, Oracle und SQL Server (wird andernfalls ignoriert). Für SQL Server gilt dieser Parameter für die primäre Datendatei und die Protokolldateien.

### **-tablespaceNamePrefix tabellenbereichspräfix**

Ein optionaler Parameter zur Angabe einer Präfixzeichenfolge, die an den Anfang von Tabellenbereichsnamen gesetzt wird, um sie eindeutig zu machen. Der Standardwert lautet `BSP`. Wenn ein Präfix für einen Tabellenbereichsnamen länger als vier Zeichen ist, wird es auf vier Zeichen abgeschnitten. Gültig für DB2, DB2 z/OS V8, DB2 z/OS V9 und Oracle (wird andernfalls ignoriert).

### **-dbLocationName datenbankpositionsname**

Ein optionaler Parameter zur Angabe der Speicherposition der Datenbank auf z/OS. Der Standardwert ist `BSP` oder der Produktdatenbankname. Gültig für DB2 z/OS V8 und V9 (wird andernfalls ignoriert).

### **-storageGroup speichergruppe**

Ein optionaler Parameter, der die Speichergruppe unter z/OS für Business Space angibt. Wenn Sie z/OS verwenden, müssen Sie die generierten Datenbankskripts vor der Ausführung aktualisieren. Weitere Informationen zu den Skripts finden Sie im Abschnitt zur Konfiguration der Business Space-Datenbanktabellen.

### **-bspacedbDesign name\_der\_datenbankentwurfsdatei**

Ein optionaler Parameter, der eine Datenbankentwurfsdatei angibt, mit deren Hilfe Sie alle Informationen zur Datenbankkonfiguration einschließlich des Schemas und des Tabellenbereichsverzeichnisses definieren. Wenn Sie eine Datenbankentwurfsdatei mithilfe des Parameters **-bspacedbDesign** festlegen, müssen Sie die Parameter **-schemaName**, **-tablespaceDir** oder **-storageGroup** nicht angeben, außer Sie wollen spezielle in der Datenbankentwurfsdatei enthaltene Informationen zur Datenbankkonfiguration überschreiben.

**Anmerkung:** Der JNDI-Name jdbc/mashupDS wird stets für eine Business Space-Datenquelle verwendet, sodass der JNDI-Name in der Datenbankentwurfsdatei nicht verwendet wird. Ist eine Datenquelle mit dem JNDI-Namen jdbc/mashupDS vorhanden, wird dieser Befehl gestoppt, ohne dass das Profil konfiguriert wird, außer Sie geben zusätzlich den Parameter `-replaceDatasource true` an.

**-productTypeForDatasource** *produktdatenbank*

Ein optionaler Parameter zur Angabe der Eigenschaften, die bei der Erstellung der Datenquelle zu verwenden sind, die mit Business Space verwendet werden soll. Bei der Angabe des Parameters **productTypeForDatasource** wird eine Datenquelle für Business Space mit dem JNDI-Namen jdbc/mashupDS erstellt, die nach der Datenquelle eines installierten Produkts wie IBM Process Server, WebSphere Enterprise Service Bus, IBM Business Monitor und WebSphere Business Compass modelliert wird. Gültige Werte sind WPS (IBM Business Process Manager oder WebSphere Enterprise Service Bus), WPBS (WebSphere Business Compass) und WBM (IBM Business Monitor). Wird außerdem der Parameter **bspacedbDesign** angegeben, überschreibt **productTypeForDatasource** den Datenbanktyp und den JDBC-Provider und der JNDI-Name in der Datenbankentwurfsdatei wird nicht verwendet.

**Anmerkung:** Ist eine Datenquelle mit dem JNDI-Namen jdbc/mashupDS vorhanden, wird dieser Befehl gestoppt, ohne dass das Profil konfiguriert wird, außer Sie geben zusätzlich den Parameter `-replaceDatasource true` an.

**-replaceDatasource true|false**

Ein optionaler Parameter, der angibt, ob der Befehl **configureBusinessSpace** ausgeführt wird, wenn das Profil bereits konfiguriert wurde. Der Standardwert ist `false` (falsch). Wird ein Profil für Business Space konfiguriert, wird eine Datenquelle mit dem JNDI-Namen jdbc/mashupDS erstellt. Wenn die Datenquelle vorhanden ist und Sie den Befehl **configureBusinessSpace** ohne Angabe von `-replaceDatasource true` ausführen, ändert der Befehl die Konfiguration nicht. Wenn Sie `true` angeben, löscht der Befehl die Datenquelle und ihren JDBC-Provider, erstellt neue Objekte und erstellt neue DDL-Scripts.

**-save true|false**

Ein Parameter, der angibt, ob Ihre Konfigurationsänderungen gespeichert werden sollen. Der Standardwert ist `false` (falsch).

## Beispiel

Im folgenden Beispiel wird der Befehl **configureBusinessSpace** zum Konfigurieren einer Business Space-Datenquelle auf einem WebSphere Portal-Server verwendet.

- Beispiel mit Jython:

```
AdminTask.configureBusinessSpace('[-nodeName myNode -serverName myServer]')
```

- Beispiel mit Jacl:

```
$AdminTask configureBusinessSpace {-nodeName myNode -serverName myServer}
```

Im folgenden Beispiel wird der Befehl **configureBusinessSpace** ausgeführt, um eine Business Space-Datenquelle in einem Cluster zu konfigurieren. Anschließend werden die Änderungen gespeichert.

- Beispiel mit Jython:

```
AdminTask.configureBusinessSpace('[-clusterName myCluster -save true]')
```



- Beispiel mit Jacl:

```
$AdminTask configureBusinessSpace {-clusterName myCluster -save true}
```

Im folgenden Beispiel wird der Befehl **configureBusinessSpace** ausgeführt, um eine Business Space-Datenquelle in einem Cluster mit einem Schemanamen und einer Produktdatenquelle zu konfigurieren, der bzw. die auf IBM Process Server ausgelegt ist.

- Beispiel mit Jython:

```
AdminTask.configureBusinessSpace('[-clusterName myCluster -schemaName myCluster -productTypeForDatasource WPS -save true]')
```

- Beispiel mit Jacl:

```
$AdminTask configureBusinessSpace {-clusterName myCluster -schemaName meinCluster -productTypeForDatasource WPS -save true}
```

Im folgenden Beispiel wird der Befehl **configureBusinessSpace** ausgeführt, um mithilfe der in der Datenbankentwurfsdatei enthaltenen Datenbankinformationen eine Business Space-Datenquelle in einem Cluster zu konfigurieren.

- Beispiel mit Jython:

```
AdminTask.configureBusinessSpace('[-clusterName myCluster -bspacedbDesign "C:/Bspace_dbDesign.properties" -save true]')
```

- Beispiel mit Jacl:

```
$AdminTask configureBusinessSpace {-clusterName myCluster -bspacedbDesign "C:/Bspace_dbDesign.properties" -save true}
```

### Befehl 'createBPMApiFederationDomain':

Mit dem Befehl **createBPMApiFederationDomain** können Sie die Föderationsdomänen in einer Umgebung mit mehreren Implementierungszielen so konfigurieren, dass Sie Prozesse und Tasks, die in Process Designer und Integration Designer erstellt wurden, in derselben Taskliste anzeigen können.

Der Befehl **createBPMApiFederationDomain** mit dem Schritt **addTarget** erstellt eine Föderationsdomäne, um Tasks und Prozesse über eines oder mehrere Implementierungsziele hinweg zusammenzufassen. Die Federation API gibt Ihnen die Möglichkeit, Prozesse und Tasks in derselben Taskliste anzuzeigen, die in Process Designer und Integration Designer erstellt wurden. Die Federation API wird automatisch mit Ihrem Produkt als Teil der REST Services Gateway-Anwendung konfiguriert. Wenn Sie diese Konfiguration für Ihre Umgebung mit mehreren Implementierungszielen ändern wollen, verwenden Sie wsadmin-Befehle zum Erstellen und Verwalten von Föderationsdomänen. Über den Schritt **addTarget** können Sie ein oder mehr Implementierungsziele zu einer Föderationsdomäne hinzufügen. Die Federation API wirkt übergreifend über alle Systeme auf den hinzugefügten Implementierungszielen.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:

```
AdminConfig.save()
```

- Jacl:

```
$AdminConfig save
```

Geben Sie die Option **-conntype NONE** an, wenn der Anwendungsserver nicht aktiv ist.

## Zielobjekt

Bereich, in dem die Föderationsdomäne erstellt werden soll. Das Zielobjekt kann anstelle der Parameter **nodeName**, **serverName** und **clusterName** verwendet werden.

## Erforderliche Parameter

### **-serverName** *servername*

Dieser Parameter gibt den Namen des Servers an, auf dem die Föderationsdomäne verwaltet werden soll. Bei Angabe dieses Parameters muss auch der Parameter **nodeName** angegeben werden. Geben Sie diesen Parameter nicht an, wenn der Parameter **clusterName** oder ein Zielobjekt angegeben wird. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich erstellt.

### **-nodeName** *knotenname*

Dieser Parameter gibt den Namen des Knotens an, auf dem die Föderationsdomäne verwaltet werden soll. Bei Angabe dieses Parameters muss auch der Parameter **serverName** angegeben werden. Geben Sie diesen Parameter nicht an, wenn der Parameter **clusterName** oder ein Zielobjekt angegeben wird. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich erstellt.

### **-clusterName** *clustername*

Dieser Parameter gibt den Namen des Clusters an, auf dem die Föderationsdomäne verwaltet werden soll. Geben Sie diesen Parameter nicht zusammen mit den Parametern **nodeName** und **serverName** oder einem Zielobjekt an. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich erstellt.

### **-name** *name\_der\_föderationsdomäne*

Der Name der neuen Föderationsdomäne, die Sie erstellen wollen. Der Name muss eindeutig sein. Dieser Parameter ist immer erforderlich.

## Erforderliche Parameter für den addTarget-Schritt

### **-targetCellName** *zellename*

Dieser Parameter gibt den Namen der Zelle an, die als Föderationsziel verwendet wird. Wenn dieser Parameter angegeben wird, die Parameter **nodeName**, **serverName** und **clusterName** aber nicht angegeben werden, fasst die Federation API alle Systeme in der Zelle zusammen.

### **-targetNodeName** *knotenname*

Dieser Parameter gibt den Namen des Knotens an, der als Föderationsziel verwendet wird. Bei Angabe dieses Parameters fasst die Federation API alle Systeme auf diesem Knoten zusammen. Bei Angabe dieses Parameters muss auch der Parameter **targetServerName** angegeben werden. Geben Sie diesen Parameter nicht zusammen mit dem Parameter **targetClusterName** an.

### **-targetServerName** *servername*

Dieser Parameter gibt den Namen des Servers an, der als Föderationsziel verwendet wird. Bei Angabe dieses Parameters fasst die Federation API alle Systeme auf diesem Server zusammen. Bei Angabe dieses Parameters muss auch der Parameter **targetNodeName** angegeben werden. Geben Sie diesen Parameter nicht zusammen mit dem Parameter **targetClusterName** an.

### **-targetClusterName** *clustername*

Dieser Parameter gibt den Namen des Clusters an, der als Föderationsziel verwendet wird. Bei Angabe dieses Parameters fasst die Federation API alle Systeme

me auf diesem Cluster zusammen. Geben Sie diesen Parameter nicht zusammen mit dem Parameter **targetNodeName** oder **targetServerName** an.

## Beispiele

Das folgende Beispiel verwendet den Befehl **createBPMApiFederationDomain**, um eine Föderationsdomäne mit dem Namen `myCustomFederationDomain` hinzuzufügen, die sich über einen Server (mit dem Knotennamen `myNode` und dem Servernamen `myServer`) und einen Cluster (mit dem Namen `myCluster`) erstreckt.

- Beispiel mit Jython:

```
AdminTask.createBPMApiFederationDomain('[-nodeName knotenname
-serverName servername -name myCustomFederationDomain
-addTarget [{" myNode myServer ""} [{" "" "" "" myCluster}]]')
```

- Beispiel mit Jacl:

```
$AdminTask createBPMApiFederationDomain {-nodeName knotenname
-serverName servername -name myCustomFederationDomain
-addTarget [{" myNode myServer ""} [{" "" "" "" myCluster}]}
```

## Befehl 'deleteBPMApiFederationDomain':

Mit dem Befehl **deleteBPMApiFederationDomain** können Sie eine Föderationsdomäne mit den enthaltenen Zielen löschen.

Dieser Befehl löscht eine Föderationsdomäne (mit den in ihr enthaltenen Zielen), die Tasks und Prozesse für eines oder mehrere Implementierungsziele zusammenfasst. Die Federation API gibt Ihnen die Möglichkeit, Prozesse und Tasks anzuzeigen, die in Process Designer und Integration Designer in derselben Taskliste erstellt wurden. Die Federation API wird automatisch mit Ihrem Produkt als Teil der REST Services Gateway-Anwendung konfiguriert. Wenn Sie diese Konfiguration für Ihre Umgebung mit mehreren Implementierungszielen ändern wollen, verwenden Sie `wsadmin`-Befehle zum Erstellen und Verwalten von Föderationsdomänen.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:

```
AdminConfig.save()
```

- Jacl:

```
$AdminConfig save
```

Geben Sie die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

## Zielobjekt

Bereich, für den die Föderationsdomäne gelöscht werden soll. Das Zielobjekt kann anstelle der Parameter **nodeName**, **serverName** und **clusterName** verwendet werden.

## Erforderliche Parameter

**-serverName** *servername*

Dieser Parameter gibt den Namen des Servers an, auf dem die Föderationsdomäne verwaltet werden soll. Bei Angabe dieses Parameters muss auch der Parameter **nodeName** angegeben werden. Geben Sie diesen Parameter nicht an, wenn der Parameter **clusterName** oder ein Zielobjekt angegeben wird. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

**-nodeName** *knotenname*

Dieser Parameter gibt den Namen des Knotens an, auf dem die Föderationsdomäne verwaltet werden soll. Bei Angabe dieses Parameters muss auch der Parameter **serverName** angegeben werden. Geben Sie diesen Parameter nicht an, wenn der Parameter **clusterName** oder ein Zielobjekt angegeben wird. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

**-clusterName** *clustername*

Dieser Parameter gibt den Namen des Clusters an, auf dem die Föderationsdomäne verwaltet werden soll. Geben Sie diesen Parameter nicht zusammen mit den Parametern **nodeName** und **serverName** oder einem Zielobjekt an. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

**-name** *name\_der\_föderationsdomäne*

Der Name der Föderationsdomäne, die Sie löschen wollen. Der Name muss eindeutig sein. Dieser Parameter ist immer erforderlich.

### Beispiel

Im folgenden Beispiel wird der Befehl **deleteBPMApiFederationDomain** verwendet, um eine Föderationsdomäne zu löschen:

- Beispiel mit Jython:

```
AdminTask.deleteBPMApiFederationDomain(['-nodeName myNode -serverName myServer -name myFederationD
```

- Beispiel mit Jacl:

```
$AdminTask deleteBPMApiFederationDomain {-nodeName myNode -serverName myServer -name myFederationD
```

### Befehl 'getBusinessSpaceDeployStatus':

Mit dem Befehl **getBusinessSpaceDeployStatus** können Sie überprüfen, ob Business Space powered by WebSphere auf einem bestimmten Implementierungsziel konfiguriert ist.

Mit diesem Befehl wird überprüft, ob Business Space auf einem angegebenen Server, Knoten oder Cluster konfiguriert ist. Wenn Sie keine Parameter angeben, wird überprüft, ob Business Space in der Zelle konfiguriert ist.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:

```
AdminConfig.save()
```

- Jacl:

```
$AdminConfig save
```

Geben Sie die Option **-conntype NONE** an, wenn der Anwendungsserver nicht aktiv ist.

### Erforderliche Parameter

**-serverName** *servername*

Dieser Parameter gibt den Servernamen an, der in Bezug auf Business Space überprüft wird.

**-nodeName** *knotenname*

Dieser Parameter gibt den Knotennamen an, der in Bezug auf Business Space überprüft wird.

**-clusterName** *clustername*

Dieser Parameter gibt den Clusternamen an, der in Bezug auf Business Space überprüft wird.

## Beispiel

Im folgenden Beispiel wird der Befehl **getBusinessSpaceDeployStatus** ausgeführt, der überprüft, ob Business Space auf einem Server konfiguriert ist.

- Beispiel mit Jython:

```
AdminTask.getBusinessSpaceDeployStatus(['-nodeName myNode -serverName myServer'])
```

- Beispiel mit Jacl:

```
$AdminTask getBusinessSpaceDeployStatus {-nodeName myNode -serverName myServer}
```

Im folgenden Beispiel wird der Befehl **getBusinessSpaceDeployStatus** ausgeführt, der überprüft, ob Business Space in einem Cluster konfiguriert ist.

- Beispiel mit Jython:

```
AdminTask.getBusinessSpaceDeployStatus(['-clusterName myCluster'])
```

- Beispiel mit Jacl:

```
$AdminTask getBusinessSpaceDeployStatus {-clusterName myCluster}
```

Im folgenden Beispiel wird der Befehl **getBusinessSpaceDeployStatus** ausgeführt, der eine Liste aller Implementierungsziele (Server und Cluster), zurückgibt, die für Business Space in einer Zelle konfiguriert wurden.

Wenn Sie den Befehl im Profilstammverzeichnis `bin` ausführen, gibt er eine Liste aller Implementierungsziele (Server und Cluster), zurück, die für Business Space in einer Zelle konfiguriert wurden.

Wenn Sie den Befehl im Installationsstammverzeichnis `bin` ausführen, gibt er eine Liste aller Implementierungsziele (Server und Cluster), zurück, die für Business Space in demselben Installationsstammverzeichnis konfiguriert wurden.

- Beispiel mit Jython:

```
AdminTask.getBusinessSpaceDeployStatus()
```

- Beispiel mit Jacl:

```
$AdminTask getBusinessSpaceDeployStatus
```

## Befehl 'installBusinessSpace':

Verwenden Sie den Befehl **installBusinessSpace**, um Business Space powered by WebSphere in der Laufzeitumgebung zu konfigurieren.

Mit dem Befehl **installBusinessSpace** können die EAR-Dateien für Business Space in der Laufzeitumgebung installiert werden. Mit dem Befehl kann darüber hinaus die Konfiguration aktualisiert werden, ohne Business Space zu installieren.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:

```
AdminConfig.save()
```

- Jacl:  
\$AdminConfig save

Geben Sie die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

### Erforderliche Parameter

Entweder sind die Parameter `-serverName` und `-nodeName` erforderlich oder es ist der Parameter `-clusterName` erforderlich.

#### **-serverName** *servername*

Dieser Parameter gibt den Servernamen für die Konfiguration an. Für die Konfiguration von Business Space auf einem Server müssen Sie die beiden Parameter **serverName** und **nodeName** angeben.

#### **-nodeName** *knotenname*

Dieser Parameter gibt den Knotennamen für die Konfiguration an. Für die Konfiguration von Business Space auf einem Server müssen Sie die beiden Parameter **serverName** und **nodeName** angeben.

#### **-clusterName** *clustername*

Dieser Parameter gibt den Clusternamen für die Konfiguration an. Für die Konfiguration von Business Space auf einem Cluster müssen Sie den Parameter **clusterName** angeben.

### Optionale Parameter

#### **-noWidgets** *true|false*

Ein optionaler Parameter, der bei der Einstellung `true` (wahr) verhindert, dass die Widgets des Produkts auf dem Implementierungsziel installiert werden. Wenn Sie später die Widgets installieren wollen, müssen Sie dazu den Befehl **installBusinessSpaceWidgets** verwenden, nachdem die Konfiguration von Business Space erfolgreich abgeschlossen wurde. Der Standardwert lautet `false`.

#### **-save** *true|false*

Ein optionaler Parameter, der angibt, ob Ihre Konfigurationsänderungen gespeichert werden sollen. Der Standardwert ist `false` (falsch).

#### **-configUpdateOnly** *true|false*

Ein optionaler Parameter, der bei Einstellung auf `true` bewirkt, dass nur die Konfiguration aktualisiert wird, ohne die Business Space-EAR-Dateien auf dem Implementierungsziel zu installieren. Der Standardwert ist `false` (falsch).

#### **-configEnv** *bpm\_adv*

Ein optionaler Parameter, der ein bestimmtes Business Space-Konfigurationsverhalten aktiviert. Wenn Sie Ihr IBM Business Process Manager Standard-Profil erweitert haben, um IBM Business Monitor einzuschließen, und Sie feststellen, dass nach der Anmeldung bei Process Portal das Globussymbol nicht angezeigt wird, mit dem Benutzer zu Business Space-Spaces wechseln können, die IBM Business Monitor-Widgets enthalten, müssen Sie den Befehl **installBusinessSpace** mit diesem Parameter und mit `-configUpdateOnly true` ausführen, um das Globussymbol zu aktivieren.



## Beispiele: Business Space installieren

Im folgenden Beispiel wird der Befehl **installBusinessSpace** ausgeführt, um EAR-Dateien für Business Space auf einem Server zu installieren.

- Jython-Beispiel:

```
AdminTask.installBusinessSpace('[-nodeName myNode -serverName  
myServer -save true]')
```

- Jacl-Beispiel:

```
$AdminTask installBusinessSpace {-nodeName myNode -serverName  
myServer -save true}
```

Im folgenden Beispiel wird der Befehl **installBusinessSpace** ausgeführt, um EAR-Dateien für Business Space in einem Cluster zu installieren.

- Jython-Beispiel:

```
AdminTask.installBusinessSpace('[-clusterName myCluster -save true]')
```

- Jacl-Beispiel:

```
$AdminTask installBusinessSpace {-clusterName myCluster -save true}
```

## Beispiele: Globussymbol in Process Portal aktivieren

Im folgenden Clusterbeispiel wird der Befehl **installBusinessSpace** zum Aktivieren des Globussymbols in Process Portal verwendet. Über dieses Symbol können Benutzer zu Business Space-Spaces wechseln, die IBM Business Monitor-Widgets enthalten. Die Business Space-EAR-Dateien werden in diesem Beispiel nicht installiert. Dieses Beispiel ist nur anwendbar, wenn Sie Ihr IBM Business Process Manager Standard-Profil erweitert haben, um IBM Business Monitor einzuschließen.

Jacl-Beispiel:

```
wsadmin>$AdminTask installBusinessSpace {-clusterName myCluster -configUpdateOnly true -configEnv
```

Jython-Beispiel:

```
AdminTask.installBusinessSpace(['-clusterName', 'myCluster', '-configUpdateOnly', 'true', '-config
```

## Befehl 'installBusinessSpaceWidgets':

Mit dem Befehl **installBusinessSpaceWidgets** können Sie Widgets zur Verwendung mit Business Space powered by WebSphere installieren, implementieren und registrieren.

Mit dem Befehl **installBusinessSpaceWidgets** werden bestimmte, in einer komprimierten Datei oder einer EAR-Datei enthaltene Widgets installiert, implementiert und registriert. Wenn bereits Widgets implementiert sind, aktualisiert **installBusinessSpaceWidgets** die Binär- und Registrierungsinformationen.

Die Struktur der komprimierten Datei eines Widgets enthält folgende Elemente:

- [ear\widgets\_name.ear] - eine oder mehrere EAR-Dateien
- [catalog\catalog\_name.xml]
- [endpoints\\*.xml] - Widgetendpunkte
- [templates\\*.zip] - Schablonen müssen in einer komprimierten Datei vorliegen und das IBM Lotus Mashups-Schablonenformat aufweisen.
- [help\eclipse\plugins\\*]

Es sind nicht alle Ordner erforderlich. Leere Ordner sind gültig.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:  
AdminConfig.save()
- Jacl:  
\$AdminConfig save

Geben Sie die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

### Erforderliche Parameter

#### **-serverName** *servername*

Dieser Parameter gibt den Servernamen für die Konfiguration an. Für die Konfiguration von Business Space auf einem Server muss ein **Servername** und ein **Knotenname** angegeben werden.

#### **-nodeName** *knotenname*

Dieser Parameter gibt den Knotennamen für die Konfiguration an. Es ist entweder ein Servername, ein Knotenname oder ein Clustername erforderlich. Für die Konfiguration von Business Space-Widgets auf einem Server müssen Sie sowohl den Parameter **serverName** als auch **nodeName** angeben.

#### **-clusterName** *clustername*

Dieser Parameter gibt den Clusternamen für die Konfiguration an. Für die Konfiguration von Business Space-Widgets in einem Cluster muss ein Parameter **clusterName** angegeben werden.

#### **-widgets** *widgetspfad*

Ein Parameter, mit dem wahlweise Folgendes angegeben wird:

- Der vollständige Pfad zu dem Verzeichnis, das die komprimierten Dateien oder die EAR-Dateien mit den Widgets enthält. Wenn Sie ein Verzeichnis angeben, werden alle Widgets für alle komprimierten Dateien und EAR-Dateien in diesem Verzeichnis installiert.
- Der vollständige Pfad zu einer einzelnen komprimierten Datei, in der die Widgets enthalten sind.
- Der vollständige Pfad zu einer einzelnen EAR-Datei, in der die Widgets enthalten sind.

#### **-save true|false**

Ein Parameter, der angibt, ob Ihre Konfiguration gespeichert werden soll. Der Standardwert ist `true` (wahr).

### Optionale Parameter

#### **-save true|false**

Ein Parameter, der angibt, ob Ihre Konfiguration gespeichert werden soll. Der Standardwert ist `true` (wahr).

### Beispiel

Im folgenden Beispiel wird der Befehl **installBusinessSpaceWidgets** ausgeführt, um Widgets auf einem Server zu installieren, zu implementieren und zu registrieren.

- Beispiel mit Jython:

```
AdminTask.installBusinessSpaceWidgets('[-nodeName knotenname  
-serverName servername -widgets  
installationsstammverzeichnis/BusinessSpace/registryData/produktname/widgets/MyWidget.zip]')
```

- Beispiel mit Jacl:

```
$AdminTask installBusinessSpaceWidgets {-nodeName knotenname  
-serverName servername -widgets  
installationsstammverzeichnis/BusinessSpace/registryData/produktname/widgets/MyWidget.zip}
```

Im folgenden Beispiel wird der Befehl **installBusinessSpaceWidgets** ausgeführt, um Widgets in einem Cluster zu installieren, zu implementieren und zu registrieren.

- Beispiel mit Jython:

```
AdminTask.installBusinessSpaceWidgets('[-clusterName clustername  
-widgets X:/WPS/Temp]')
```

- Beispiel mit Jacl:

```
$AdminTask installBusinessSpaceWidgets {-clusterName clustername  
-widgets X:/WPS/Temp}
```

Nachdem die Befehle **installBusinessSpaceWidgets** oder **updateBusinessSpaceWidgets** ausgeführt wurden, sind manuelle Schritte zur Aktualisierung von Business Space-Vorlagen und Spaces erforderlich. Weitere Informationen finden Sie im Abschnitt Aktualisierung von Business Space-Vorlagen und Spaces nach der Installation oder Aktualisierung von Widgets.

### Befehl **installHumanTaskManagementWidgets**:

Verwenden Sie den Befehl **installHumanTaskManagementWidgets**, um die Widgetanwendung zur Benutzertaskverwaltung auf einem IBM BPM Standard- oder IBM BPM Advanced-Server bzw. -Cluster zu installieren.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced ohne konfigurierten Business Space

Wenn Sie Widgets zur Benutzertaskverwaltung in einer zellenübergreifenden Konfiguration mit IBM Case Manager verwenden möchten, nehmen Sie den Befehl **installHumanTaskManagementWidgets**, um nur die erforderliche Widgetanwendung zu installieren.

### Erforderliche Parameter

#### **-clusterName** *clustername*

Dieser Parameter gibt den Namen des IBM BPM-Clusters an, in dem die Widgetanwendung zur Benutzertaskverwaltung installiert wird. Normalerweise sollte es sich dabei um den Cluster handeln, in dem Business Space installiert wäre. Beispiel: den Anwendungscluster in einer Topologie mit einem oder zwei Clustern, den Unterstützungscluster in einer Topologie mit drei Clustern und den Webanwendungscluster in einer Topologie mit vier Clustern.

Wenn Sie den Parameter **clusterName** angeben, dann geben nicht zugleich die beiden Parameter **serverName** und **nodeName** an.

#### **-nodeName** *knotenname*

Dieser Parameter gibt den Namen des IBM BPM-Knotens an, in dem die Widgetanwendung zur Benutzertaskverwaltung installiert ist. Wenn Sie den Parameter **clusterName** nicht angeben, müssen Sie die beiden Parameter **serverName** und **nodeName** setzen.

#### **-serverName** *servername*

Dieser Parameter gibt den Namen des IBM BPM-Servers an, in dem die Widgetanwendung zur Benutzertaskverwaltung installiert wird. Wenn Sie Business Space später auf dem selben Server konfigurieren, auf dem die Widgetanwendung zur Benutzertaskverwaltung installiert ist, wird die vorhandene Anwendung dann von Business Space verwendet. Wenn Sie den Parameter **clusterName** nicht angeben, müssen Sie die beiden Parameter **serverName** und **nodeName** setzen.

#### **Beispiel**

Im folgenden Beispiel wird der Befehl **installHumanTaskManagementWidgets** verwendet, um die Widgetanwendung zur Benutzertaskverwaltung auf dem Support-Cluster zu installieren.

Beispiel mit Jython:

```
AdminTask.installHumanTaskManagementWidgets('-clusterClusterName Support')
AdminConfig.save()
```

Beispiel mit Jacl:

```
$AdminTask installHumanTaskManagementWidgets {-clusterClusterName Support}
$AdminConfig save
```

#### **Befehl 'listBPMApiFederationDomains':**

Mit dem Befehl **listBPMApiFederationDomains** können Sie alle Föderationsdomänen für Ihre Umgebung auflisten.

Dieser Befehl listet alle Föderationsdomänen auf, die für einen Server oder Cluster bestehen. Die Federation API gibt Ihnen die Möglichkeit, Prozesse und Tasks anzuzeigen, die in Process Designer und Integration Designer in derselben Taskliste erstellt wurden. Die Federation API wird automatisch mit Ihrem Produkt als Teil der REST Services Gateway-Anwendung konfiguriert. Wenn Sie diese Konfiguration für Ihre Umgebung mit mehreren Implementierungszielen ändern wollen, verwenden Sie wsadmin-Befehle zum Erstellen und Verwalten von Föderationsdomänen.

Geben Sie die Option **-conntype NONE** an, wenn der Anwendungsserver nicht aktiv ist.

#### **Zielobjekt**

Bereich, in dem die Föderationsdomäne verwaltet werden soll. Das Zielobjekt kann anstelle der Parameter **nodeName**, **serverName** und **clusterName** verwendet werden.

#### **Erforderliche Parameter**

##### **-serverName** *servername*

Dieser Parameter gibt den Namen des Servers an, auf dem die Föderationsdomäne verwaltet werden soll. Bei Angabe dieses Parameters muss auch der Parameter **nodeName** angegeben werden. Geben Sie diesen Parameter nicht an, wenn der Parameter **clusterName** oder ein Zielobjekt angegeben wird. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

##### **-nodeName** *knotenname*

Dieser Parameter gibt den Namen des Knotens an, auf dem die Föderationsdomäne verwaltet werden soll. Bei Angabe dieses Parameters muss auch der Pa-

parameter **serverName** angegeben werden. Geben Sie diesen Parameter nicht an, wenn der Parameter **clusterName** oder ein Zielobjekt angegeben wird. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

#### **-clusterName** *clustername*

Ein Parameter, der den Namen des Clusters angibt, auf dem die Föderationsdomäne verwaltet werden soll. Geben Sie diesen Parameter nicht zusammen mit den Parametern **nodeName** und **serverName** oder einem Zielobjekt an. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

### Beispiel

Im folgenden Beispiel wird der Befehl **listBPMApiFederationDomains** verwendet, um alle Föderationsdomänen auf einem Server aufzulisten.

- Beispiel mit Jython:

```
AdminTask.listBPMApiFederationDomains('[-nodeName myNode -serverName myServer]')
```

- Beispiel mit Jacl:

```
$AdminTask listBPMApiFederationDomains {-nodeName myNode -serverName myServer}
```

### Befehl 'modifyBPMApiFederationDomain':

Mit dem Befehl **modifyBPMApiFederationDomain** können Sie unter Verwendung der Schritte 'addTarget' und 'deleteTarget' Ziele zur Föderationsdomäne hinzufügen bzw. aus ihr entfernen.

Dieser Befehl fügt Ziele zu einer Föderationsdomäne hinzu oder entfernt Ziele aus ihr. Die Federation API wird automatisch mit Ihrem Produkt als Teil der REST Services Gateway-Anwendung konfiguriert. Wenn Sie diese Konfiguration für Ihre Umgebung mit mehreren Implementierungszielen ändern wollen, verwenden Sie wsadmin-Befehle zum Erstellen und Verwalten von Föderationsdomänen. Über den Schritt **addTarget** können Sie ein oder mehr Implementierungsziele zu einer Föderationsdomäne hinzufügen. Über den Schritt **deleteTarget** können Sie ein oder mehr Implementierungsziele aus einer Föderationsdomäne löschen. Die Federation API wirkt übergreifend über alle Systeme auf den hinzugefügten Implementierungszielen.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:

```
AdminConfig.save()
```

- Jacl:

```
$AdminConfig save
```

Geben Sie die Option **-conntype NONE** an, wenn der Anwendungsserver nicht aktiv ist.

### Zielobjekt

Bereich, in dem die Föderationsdomäne verwaltet werden soll. Das Zielobjekt kann anstelle der Parameter **nodeName**, **serverName** und **clusterName** verwendet werden.

## Erforderliche Parameter

### **-serverName** *servername*

Dieser Parameter gibt den Namen des Servers an, auf dem die Föderationsdomäne verwaltet werden soll. Bei Angabe dieses Parameters muss auch der Parameter **nodeName** angegeben werden. Geben Sie diesen Parameter nicht an, wenn der Parameter **clusterName** oder ein Zielobjekt angegeben wird. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

### **-nodeName** *knotenname*

Dieser Parameter gibt den Namen des Knotens an, auf dem die Föderationsdomäne verwaltet werden soll. Bei Angabe dieses Parameters muss auch der Parameter **serverName** angegeben werden. Geben Sie diesen Parameter nicht an, wenn der Parameter **clusterName** oder ein Zielobjekt angegeben wird. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

### **-clusterName** *clustername*

Dieser Parameter gibt den Namen des Clusters an, auf dem die Föderationsdomäne verwaltet werden soll. Geben Sie diesen Parameter nicht zusammen mit den Parametern **nodeName** und **serverName** oder einem Zielobjekt an. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

### **-name** *name\_der\_föderationsdomäne*

Der Name der neuen Föderationsdomäne, die Sie ändern wollen. Der Name muss eindeutig sein. Dieser Parameter ist immer erforderlich.

## Erforderliche Parameter für die Schritte 'addTarget' und 'deleteTarget'

### **-targetCellName** *zellename*

Dieser Parameter gibt den Namen der Zelle an, die als Föderationsziel verwendet wird. Wenn dieser Parameter angegeben wird, die Parameter 'nodeName', 'serverName' und 'clusterName' aber nicht angegeben werden, fasst die Federation API alle Systeme in der Zelle zusammen.

### **-targetNodeName** *knotenname*

Dieser Parameter gibt den Namen des Knotens an, der als Föderationsziel verwendet wird. Bei Angabe dieses Parameters fasst die Federation API alle Systeme auf diesem Server zusammen. Wenn der Parameter angegeben wird, muss auch der Parameter 'targetServerName' angegeben werden. Geben Sie diesen Parameter nicht zusammen mit dem Parameter 'targetClusterName' an.

### **-targetServerName** *servername*

Dieser Parameter gibt den Namen des Servers an, der als Föderationsziel verwendet wird. Bei Angabe dieses Parameters fasst die Federation API alle Systeme auf diesem Server zusammen. Wenn der Parameter angegeben wird, muss auch der Parameter 'targetNodeName' angegeben werden. Geben Sie diesen Parameter nicht zusammen mit dem Parameter 'targetClusterName' an.

### **-targetClusterName** *clustername*

Dieser Parameter gibt den Namen des Servers an, der als Föderationsziel verwendet wird. Bei Angabe dieses Parameters fasst die Federation API alle Systeme auf diesem Cluster zusammen. Geben Sie diesen Parameter nicht zusammen mit dem Parameter 'targetNodeName' oder 'targetServerName' an.



## Beispiele

Im folgenden Beispiel wird der Befehl **modifyBPMApiFederationDomain** verwendet, um das Implementierungsziel mit myNode, myServer zu löschen und um ein neues Implementierungsziel myNewNode, myNewServer hinzuzufügen.

- Beispiel mit Jython:

```
AdminTask.modifyBPMApiFederationDomain(['-nodeName knotenname  
-serverName servername -name myCustomFederationDomain  
-deleteTarget [{" myNode myServer ""}]')  
-addTarget [{" myNewNode myNewServer ""}]']')
```

- Beispiel mit Jacl:

```
$AdminTask modifyBPMApiFederationDomain {-nodeName knotenname  
-serverName servername -name myCustomFederationDomain  
-deleteTarget [{" myNode myServer ""}]  
-addTarget [{" myNewNode myNewServer ""}]}
```

## Befehl 'registerRESTServiceEndpoint':

Mit dem Befehl **registerRESTServiceEndpoint** können Sie konfigurierte und aktivierte REST-Endpunkte so registrieren, dass Ihr Team die Widgets in Business Space verwenden kann.

Mit diesem Befehl werden die REST-Serviceendpunkte so registriert, dass Business Space ordnungsgemäß mit Widgets für Ihr Produkt verbunden wird. Dieser Befehl registriert die Endpunkte der REST-Services, die sich in derselben Zelle wie Business Space befinden.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:

```
AdminConfig.save()
```

- Jacl:

```
$AdminConfig save
```

Geben Sie die Option **-conntype NONE** an, wenn der Anwendungsserver nicht aktiv ist.

## Erforderliche Parameter

**-clusterName** *name\_des\_rest\_service\_clusters*

Dieser Parameter gibt den Clusternamen für den REST-Service an. Bei der Registrierung von REST-Serviceendpunkten für einen Cluster müssen Sie den Parameter **clusterName** angeben.

**-nodeName** *name\_des\_rest\_serviceknotens*

Dieser Parameter gibt den Knotennamen für den REST-Service an. Bei der Registrierung von REST-Serviceendpunkten für einen Server müssen Sie sowohl den Parameter **serverName** als auch **nodeName** angeben.

**-serverName** *name\_des\_rest\_service\_servers*

Dieser Parameter gibt den Servernamen für den REST-Service an. Bei der Registrierung von REST-Serviceendpunkten für einen Server müssen Sie sowohl den Parameter **serverName** als auch **nodeName** angeben.

- businessSpaceClusterName** *name\_des\_business\_space\_clusters*  
Der Name des Business Space-Clusters. Wenn Business Space in einem Cluster konfiguriert wird, müssen Sie den Parameter **businessSpaceClusterName** angeben.
- businessSpaceNodeName** *name\_des\_business\_space\_knotens*  
Der Name des Business Space-Knotens. Wenn Business Space auf einem Server konfiguriert wird, müssen Sie sowohl den Parameter **businessSpaceServerName** als auch **businessSpaceNodeName** angeben.
- businessSpaceServerName** *name\_des\_business\_space\_servers*  
Der Name des Business Space-Servers. Wenn Business Space auf einem Server konfiguriert wird, müssen Sie sowohl den Parameter **businessSpaceServerName** als auch **businessSpaceNodeName** angeben.

### Optionale Parameter

- appName** *name\_der\_providieranwendung*  
Der Anwendungsname des REST-Service-Providers.
- name** *name\_des\_rest-service*  
Der Name des REST-Service.
- type** *name\_des\_servicetyps*  
Der Typ des Service. Dieser Parameter ist optional. Wird dieser Parameter nicht angegeben, werden alle eindeutigen REST-Serviceendpunkte registriert, die für einen angegebenen REST-Service-Provider in einem angegebenen Implementierungsziel konfiguriert wurden. Wenn Sie einen bestimmten Serviceendpunkt angeben möchten, verwenden Sie den Wert `<tns:type>`, der sich in der Endpunktdatei für ein Widget befindet. Die Serviceendpunktdateien befinden sich im Verzeichnis `installationsstammverzeichnis\BusinessSpace\registryData\produktname\endpoints`. So enthält zum Beispiel `bpmAdministrationEndpoints.xml` alle Serviceendpunkttypen, die von Widgets 'Verwaltung' verwendet werden. Der Wert des Elements `<tns:type>` ist `{com.ibm.bpm}SCA`:

```
<tns:Endpoint>
  <tns:id>{com.ibm.bpm}SCA</tns:id>
  <tns:type>{com.ibm.bpm}SCA</tns:type>
  <tns:version>6.2.0.0</tns:version>
  <tns:url>/rest/sca/v1</tns:url>
  <tns:description>Location backend SCA REST Services
  for Module Administration widgets and Service Monitoring widget
</tns:description>
</tns:Endpoint>
```

Stellen Sie bei Jacl sicher, dass Sie den Wert in doppelte Anführungszeichen einschließen. Beispiel: `... -type "{com.ibm.bpm}SCA" ....`

- version** *versionsname*  
Die Version des REST-Service-Providers.
- webModuleName** *name\_des\_webmoduls*  
Der Webmodulname des REST-Service-Providers.

### Beispiel

Im folgenden Beispiel wird der Befehl **registerRESTServiceEndpoint** verwendet. Alle konfigurierten und aktivierten REST-Services in dem Cluster werden bei Business Space registriert.

- Beispiel mit Jython:

```
AdminTask.registerRESTServiceEndpoint('[-clusterName
name_des_rest-services-cluster -businessSpaceClusterName
name_des_business_space-clusters]')
```

- Beispiel mit Jacl:

```
$AdminTask registerRESTServiceEndpoint {-clusterName
name_des_rest-services-cluster -businessSpaceClusterName
name_des_business_space-clusters}
```

### Befehl **removeICMSystem**:

Verwenden Sie den Befehl **removeICMSystem** zur Entfernung von Endpunkten für IBM Case Manager-Services aus der Endpunktregistrierungsdatei für IBM BPM.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

Dieser Befehl muss dort ausgeführt werden, wo die IBM BPM eingebundene REST API implementiert ist. Geben Sie die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

Obwohl der Befehl **addICMSystem** zum Hinzufügen eines IBM Case Manager-Systems zu einer Föderationsdomäne verwendet werden kann, ist es nicht umgekehrt möglich, den Befehl **removeICMSystem** zum Entfernen eines Implementierungsziels aus einer Föderationsdomäne zu verwenden. Für diese Task dienen die Verwaltungsbefehle für Föderationsdomänen.

### Erforderliche Parameter

**-icmCellName** *zellename*

Ein Parameter, der den Namen der IBM Case Manager-Zelle angibt.

**-icmNodeName** *knotenname*

Ein Parameter, der den Namen des IBM Case Manager-Knotens angibt. Geben Sie entweder die beiden Parameter **icmServerName** und **icmNodeName** an oder nur den Parameter **icmClusterName**.

**-icmServerName** *servername*

Ein Parameter, der den Namen des IBM Case Manager-Servers angibt. Geben Sie entweder die beiden Parameter **icmServerName** und **icmNodeName** an oder nur den Parameter **icmClusterName**.

**-icmClusterName** *clustername*

Ein Parameter, der den Namen des IBM Case Manager-Clusters angibt. Geben Sie entweder die beiden Parameter **icmServerName** und **icmNodeName** an oder nur den Parameter **icmClusterName**.

**-PEConnectionName** *verbindungsname*

Ein Parameter, der den Verbindungsnamen für die Prozessengine von IBM Case Manager angibt.

### Beispiel

Das folgende Beispiel verwendet den Befehl **removeICMSystem** zum Entfernen der IBM Case Manager-Endpunkte für IBM Case Manager-Services in einem Cluster.

Beispiel mit Jython:

```
AdminTask.removeICMSystem('[-icmCellName zellename  
-icmClusterName clustername  
-PEConnectionName verbindungsname')
```

Beispiel mit Jacl:

```
$AdminTask removeICMSystem {-icmCellName zellename  
-icmClusterName clustername  
-PEConnectionName verbindungsname}
```

### Befehl 'showBPMApiFederationDomain':

Mit dem Befehl **showBPMApiFederationDomain** können Details zu einer Föderationsdomäne angezeigt werden.

Dieser Befehl zeigt Details über die Ziele, die konfiguriert werden, sowie zu dem Knoten, Server und Cluster einer bestimmten Föderationsdomäne an. Die Federation API wird automatisch mit Ihrem Produkt als Teil der REST Services Gateway-Anwendung konfiguriert. Wenn Sie diese Konfiguration für Ihre Umgebung mit mehreren Implementierungszielen ändern wollen, verwenden Sie wsadmin-Befehle zum Erstellen und Verwalten von Föderationsdomänen.

Geben Sie die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

### Zielobjekt

Bereich, in dem die Föderationsdomäne verwaltet werden soll. Das Zielobjekt kann anstelle der Parameter **nodeName**, **serverName** und **clusterName** verwendet werden.

### Erforderliche Parameter

#### **-serverName** *servername*

Dieser Parameter gibt den Namen des Servers an, auf dem die Föderationsdomäne verwaltet werden soll. Bei Angabe dieses Parameters muss auch der Parameter **nodeName** angegeben werden. Geben Sie diesen Parameter nicht an, wenn der Parameter **clusterName** oder ein Zielobjekt angegeben wird. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

#### **-nodeName** *knotenname*

Dieser Parameter gibt den Namen des Knotens an, auf dem die Föderationsdomäne verwaltet werden soll. Bei Angabe dieses Parameters muss auch der Parameter **serverName** angegeben werden. Geben Sie diesen Parameter nicht an, wenn der Parameter **clusterName** oder ein Zielobjekt angegeben wird. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

#### **-clusterName** *clustername*

Dieser Parameter gibt den Namen des Clusters an, auf dem die Föderationsdomäne verwaltet werden soll. Geben Sie diesen Parameter nicht zusammen mit den Parametern **nodeName** und **serverName** oder einem Zielobjekt an. Wird kein Implementierungsziel angegeben, dann wird die Föderationsdomäne im Zellenbereich verwaltet.

#### **-name** *name\_der\_föderationsdomäne*

Der Name der Föderationsdomäne, die Sie anzeigen wollen. Der Name muss eindeutig sein. Dieser Parameter ist immer erforderlich.

## Beispiel

Im folgenden Beispiel wird der Befehl **showBPMapiFederationDomain** verwendet, um Details zu einer Föderationsdomäne anzuzeigen.

- Beispiel mit Jython:

```
AdminTask.showBPMapiFederationDomain('[-nodeName myNode -serverName  
myServer -name myFederationDomain]')
```

- Beispiel mit Jacl:

```
$AdminTask showBPMapiFederationDomain {-nodeName myNode -serverName  
myServer -name myFederationDomain}
```

## Befehl 'uninstallBusinessSpaceWidgets':

Mit dem Befehl **uninstallBusinessSpaceWidgets** können Sie Widgets und Widgetdefinitionen aus dem Profil entfernen sowie einzelne Widgetressourcen (wie Anwendungen, Kataloge, Endpunkte, Spaces, Vorlagen und Hilfetexte) entfernen.

Mit dem Befehl **uninstallBusinessSpaceWidgets** werden Widgetdateien in einer angegebenen komprimierten Datei oder einer EAR-Datei aktualisiert. Die Struktur der komprimierten Datei eines Widgets enthält folgende Elemente:

- [ear\widgets\_name.ear] - eine oder mehrere EAR-Dateien
- [catalog\catalog\_name.xml]
- [endpoints\\*.xml] - Widgetendpunkte
- [templates\\*.zip] - Schablonen müssen in einer komprimierten Datei vorliegen und das IBM Lotus Mashups-Schablonenformat aufweisen.
- [help\eclipse\plugins\\*]

Es sind nicht alle Ordner erforderlich. Leere Ordner sind gültig.

**Anmerkung:** Falls Sie die REST-Endpunktinformationen ohne den Befehl **updateBusinessSpaceWidgets** konfiguriert haben, gehen diese Endpunktänderungen nach dem Ausführen des Befehls **uninstallBusinessSpaceWidgets** verloren.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:

```
AdminConfig.save()
```

- Jacl:

```
$AdminConfig save
```

Geben Sie die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

## Erforderliche Parameter

### **-serverName** *servername*

Dieser Parameter gibt den Servernamen für die Konfiguration an. Für die Konfiguration von Business Space auf einem Server muss ein **Servername** und ein **Knotenname** angegeben werden.

### **-nodeName** *knotenname*

Dieser Parameter gibt den Knotennamen für die Konfiguration an. Für die Konfiguration von Business Space auf einem Server muss ein **Servername** und ein **Knotenname** angegeben werden.

**-clusterName** *clustername*

Dieser Parameter gibt den Clusternamen für die Konfiguration an. Für die Konfiguration von Business Space in einem Cluster muss ein **Clustername** angegeben werden.

**-widgets** *widgetspfad*

Ein Parameter, mit dem wahlweise Folgendes angegeben wird:

- Der vollständige Pfad zu dem Verzeichnis, das die komprimierten Dateien oder die Widget-EAR-Dateien mit den Widgets enthält. Wenn Sie ein Verzeichnis angeben, werden alle Widgets für alle komprimierten Dateien und EAR-Dateien in diesem Verzeichnis installiert.
- Der vollständige Pfad zu einer einzelnen komprimierten Datei, in der die Widgets enthalten sind.
- Der vollständige Pfad zu einer einzelnen EAR-Datei, in der die Widgets enthalten sind.

**Optionale Parameter**

**-save true|false**

Ein Parameter, der angibt, ob Ihre Konfigurationsänderungen gespeichert werden sollen. Der Standardwert ist true (wahr).

**Beispiel**

Im folgenden Beispiel wird der Befehl **uninstallBusinessSpaceWidgets** ausgeführt, um Widgets aus einem Cluster zu entfernen.

**Anmerkung:** Die Beispiele dienen nur der Anschaulichkeit. Sie enthalten variable Werte und sind nicht für eine Verwendung als Code-Snippets vorgesehen.

- Beispiel mit Jython:

```
AdminTask.uninstallBusinessSpaceWidgets('[-clusterName  
clustername -widgets X:/WPS/Temp]')
```

- Beispiel mit Jacl:

```
$AdminTask uninstallBusinessSpaceWidgets {-clusterName  
clustername -widgets X:/WPS/Temp}
```

**Befehl 'updateBusinessSpaceWidgets':**

Mit dem Befehl **updateBusinessSpaceWidgets** können Sie zuvor konfigurierte Business Space-Widgets sowie deren Endpunkte, Kataloge, Schablonen und Hilfe-Plugins aktualisieren.

Mit dem Befehl **updateBusinessSpaceWidgets** werden Binärdateien, Katalogdateien, Endpunktdateien, Schablonen und Hilfe-Plugins für Widgets aktualisiert, die zuvor für Business Space installiert und konfiguriert wurden.

Mit dem Befehl **updateBusinessSpaceWidgets** werden Widgetdateien in einer angegebenen komprimierten Datei oder einer EAR-Datei aktualisiert. Die Struktur der komprimierten Datei eines Widgets enthält folgende Elemente:

- [ear\widgets\_*name*.ear] - eine oder mehrere EAR-Dateien
- [catalog\catalog\_*name*.xml]
- [endpoints\\*.xml] - Widgetendpunkte
- [templates\\*.zip] - Schablonen müssen in einer komprimierten Datei vorliegen und das IBM Lotus Mashups-Schablonenformat aufweisen.
- [help\eclipse\plugins\\*]



Es sind nicht alle Ordner erforderlich. Leere Ordner sind gültig.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:  
AdminConfig.save()
- Jacl:  
\$AdminConfig save

Geben Sie die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

### Erforderliche Parameter

#### **-serverName** *servername*

Dieser Parameter gibt den Servernamen für die Konfiguration an. Für die Konfiguration von Business Space-Widgets auf einem Server müssen Sie sowohl den Parameter **serverName** als auch **nodeName** angeben.

#### **-nodeName** *knotenname*

Dieser Parameter gibt den Knotennamen für die Konfiguration an. Es ist entweder ein Servername, ein Knotenname oder ein Clustername erforderlich. Für die Konfiguration von Business Space-Widgets auf einem Server müssen Sie sowohl den Parameter **serverName** als auch **nodeName** angeben.

#### **-clusterName** *clustername*

Dieser Parameter gibt den Clusternamen für die Konfiguration an. Für die Konfiguration von Business Space in einem Cluster muss ein **Clustername** angegeben werden.

### Optionale Parameter

#### **-widgets** *widgetpfad*

Ein Parameter, der den vollständigen Pfad zu dem Verzeichnis angibt, in dem sich die EAR-Dateien oder die komprimierten Dateien der Widgets befinden, oder den vollständigen Pfad zu einer bestimmten EAR-Datei oder komprimierten Widgetdatei.

#### **-endpoints** *endpunktpfad*

Ein Parameter, der den vollständigen Pfad zu dem Verzeichnis angibt, in dem sich die Endpunktdateien der Widgets befinden, oder den vollständigen Pfad zu einer bestimmten Endpunktdatei.

#### **-catalogs** *katalogpfad*

Ein Parameter, der den vollständigen Pfad zu dem Verzeichnis angibt, in dem sich die Katalogdateien der Widgets befinden, oder den vollständigen Pfad zu einer bestimmten Katalogdatei.

#### **-templates** *schablonenpfad*

Ein Parameter, der den vollständigen Pfad zu dem Verzeichnis angibt, in dem sich die Schablonendateien der Widgets befinden, oder den vollständigen Pfad zu einer bestimmten Schablonendatei.

#### **-helpplugins** *hilfepfad*

Ein Parameter, der den vollständigen Pfad zu dem Verzeichnis angibt, in dem sich die Onlinehilfe-Plug-in-Dateien der Widgets befinden, oder den vollständigen Pfad zur Onlinehilfe-Plug-in-Datei eines bestimmten Widgets.

**-noWidgets true|false**

Gibt an, dass Sie die Widget-EAR-Dateien, die in der komprimierten Widgetdatei enthalten sind, nicht aktualisieren möchten.

**-noEndpoints true|false**

Gibt an, dass Sie die angegebenen Endpunktdateien, die in der komprimierten Widgetdatei enthalten sind, nicht aktualisieren möchten.

**-noCatalogs true|false**

Gibt an, dass Sie die Katalogdefinitionsdateien, die in der komprimierten Widgetdatei enthalten sind, nicht aktualisieren möchten.

**-noTemplates true|false**

Gibt an, dass Sie die Vorlagen, die in der komprimierten Widgetdatei enthalten sind, nicht aktualisieren möchten.

**-noHelp true|false**

Gibt an, dass Sie die Hilfedateien, die in der komprimierten Widgetdatei enthalten sind, nicht aktualisieren möchten.

**-save true|false**

Ein Parameter, der angibt, ob Ihre Konfiguration gespeichert werden soll. Der Standardwert ist true (wahr).

## Beispiel

Im folgenden Beispiel werden Widgets mit dem Befehl **updateBusinessSpaceWidgets** in einem Cluster aktualisiert.

Beispiel mit Jython:

```
AdminTask.updateBusinessSpaceWidgets('[-clusterName clustername  
-widgets widgetpfad']')
```

Beispiel mit Jacl:

```
$AdminTask updateBusinessSpaceWidgets {-clusterName clustername  
-widgets widgetpfad}
```

Im folgenden Beispiel werden Widgets mit dem Befehl **updateBusinessSpaceWidgets** auf einem Server aktualisiert.

Beispiel mit Jython:

```
AdminTask.updateBusinessSpaceWidgets('[-nodeName knotenname  
-serverName servername -widgets widgetpfad']')
```

Beispiel mit Jacl:

```
$AdminTask updateBusinessSpaceWidgets {-nodeName knotenname  
-serverName servername -widgets widgetpfad}
```

Nachdem die Befehle **installBusinessSpaceWidgets** oder **updateBusinessSpaceWidgets** ausgeführt wurden, sind manuelle Schritte zur Aktualisierung von Business Space-Vorlagen und Spaces erforderlich. Weitere Informationen finden Sie im Abschnitt Aktualisierung von Business Space-Vorlagen und Spaces nach der Installation oder Aktualisierung von Widgets.

## Befehl 'updateRESTGatewayService':

Mit dem Befehl **updateRESTGatewayService** können Sie einen REST-Gateway-Service so aktualisieren, dass die REST-Services konfiguriert und aktiviert werden.

Mit diesem Befehl wird der REST-Gateway-Service so aktualisiert, dass die REST-Services konfiguriert und aktiviert werden. Die Implementierung der REST-Services wird in einem eigenständigen Serverprofil automatisch ausgeführt. Für andere Konfigurationstypen können Sie auf der Seite der Administrationskonsole für REST-Services oder mit dem Befehl **updateRESTGatewayService** die REST-Services für alle Widgets Ihres Produkts in Business Space konfigurieren.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:  
`AdminConfig.save()`
- Jacl:  
`$AdminConfig save`

Geben Sie die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

### Erforderliche Parameter

#### **-clusterName** *clustername*

Dieser Parameter gibt den Clusternamen für den REST-Service an. Für die Konfiguration von REST-Services in einem Cluster muss ein Parameter **clusterName** angegeben werden.

#### **-nodeName** *knotenname*

Dieser Parameter gibt den Knotennamen für den REST-Service an. Für die Konfiguration von REST-Services auf einem Server müssen Sie sowohl den Parameter **serverName** als auch **nodeName** angeben.

#### **-serverName** *servername*

Dieser Parameter gibt den Servernamen für den REST-Service an. Für die Konfiguration von REST-Services auf einem Server müssen Sie sowohl den Parameter **serverName** als auch **nodeName** angeben.

#### **-enable** *true | false*

Gibt an, ob der REST-Service aktiviert wird. Gültige Werte: `true` (wahr) oder `false` (falsch).

### Optionale Parameter

#### **-type** *name\_des\_servicetyps*

Der Typ des REST-Service.

#### **-version** *versionsname*

Die Version des REST-Service.

### Beispiel

Im folgenden Beispiel wird der Befehl **updateRESTGatewayService** ausgeführt, um den REST-Gateway-Service so zu aktualisieren, dass die REST-Services konfiguriert und aktiviert werden.

- Beispiel mit Jython:

```
AdminTask.updateRESTGatewayService('[-nodeName node1 -serverName  
server1 -type "{com.ibm.bpm}TimeTable" -version 6.2.0.0 -enable  
true]')
```

- Beispiel mit Jacl:

```
$AdminTask updateRESTGatewayService {-nodeName node1 -serverName  
server1 -type "{com.ibm.bpm}TimeTable" -version 6.2.0.0 -enable true}
```

## Aktualisierung von Business Space-Vorlagen und Spaces nach der Installation oder Aktualisierung von Widgets:

Nachdem die Befehle **installBusinessSpaceWidgets** oder **updateBusinessSpaceWidgets** in einer Clusterumgebung ausgeführt wurden, sind manuelle Schritte zur Aktualisierung von Business Space-Vorlagen und Spaces erforderlich.

Sie müssen die folgenden zusätzlichen Schritte ausführen, wenn Sie zuvor die Befehle **installBusinessSpaceWidgets** oder **updateBusinessSpaceWidgets** verwendet haben.

1. Wird Business Space in einem Cluster konfiguriert, führen Sie die folgenden Schritte aus:
  - a. Geben Sie für die Eigenschaftendatei `oobLoadedStatus.properties` das benutzerdefinierte Profil an:
    - 1) Öffnen Sie im Deployment Manager-Profil die Datei `stammverzeichnis_des_deployment_manager-profils\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties`.
    - 2) Suchen Sie in den Eigenschaften `com.ibm.mashups.directory.templates` oder `com.ibm.mashups.directory.spaces` nach den Namen für Zelle, Knoten und Server.  
Sie können z. B. in `com.ibm.mashups.directory.templates = config/cells/Cell01/nodes/Node01/servers/Server1/mm/templates` das benutzerdefinierte Profil anhand des Zellennamens `Cell01` und des Knotennamens `Node01` finden.
    - 3) Verwenden Sie die Namen von Zelle, Knoten und Server, um das benutzerdefinierte Profil zu suchen.
  - b. Öffnen Sie im benutzerdefinierten Profil die Datei `stammverzeichnis_des_benutzerdefinierten_profils\BusinessSpace\clustername\mm.runtime.prof\public\oobLoadedStatus.properties` und aktualisieren Sie die Eigenschaften `importTemplates.txt` oder `importSpaces.txt`:

```
importTemplates.txt=true
importSpaces.txt=true
```

Wenn Sie die Business Space-Datenbank erneut erstellt haben, nachdem sie gelöscht worden war, oder wenn Sie das Thema (Motiv/Schema) aus einem anderen Grund erneut laden müssen, aktualisieren Sie auch die folgende Eigenschaft:

```
importThemes.txt=true
```
  - c. Resynchronisieren Sie das benutzerdefinierte Profil.
    - 1) Öffnen Sie die Administrationskonsole und klicken Sie auf **Systemadministration > Knoten**.
    - 2) Klicken Sie auf **Vollständige Neusynchronisation**.
  - d. Starten Sie den Cluster erneut.
2. Wird Business Space auf einem verwalteten Server konfiguriert, führen Sie die folgenden Schritte aus:
  - a. Öffnen Sie im benutzerdefinierten Profil, in dem sich der verwaltete Server befindet, die Datei `stammverzeichnis_des_benutzerdefinierten_profils\BusinessSpace\knotenname\servername\mm.runtime.prof\public\oobLoadedStatus.properties` und aktualisieren Sie die Eigenschaften `importTemplates.txt` oder `importSpaces.txt`:

```
importTemplates.txt=true
importSpaces.txt=true
```

Wenn Sie die Business Space-Datenbank erneut erstellt haben, nachdem sie gelöscht worden war, oder wenn Sie das Thema (Motiv/Schema) aus einem anderen Grund erneut laden müssen, aktualisieren Sie auch die folgende Eigenschaft:

```
importThemes.txt=true
```

- b. Resynchronisieren Sie das benutzerdefinierte Profil.
  - 1) Öffnen Sie die Administrationskonsole und klicken Sie auf **Systemadministration > Knoten**.
  - 2) Klicken Sie auf **Vollständige Neusynchronisation**.
- c. Starten Sie den Server erneut.

## Business Space-Ajax-Proxy konfigurieren

Sie können den Business Space-Ajax-Proxy für besondere Szenarios konfigurieren. Beispielsweise können Sie für sichere Produktionsumgebungen die Einstellung für die Zeitlimitüberschreitung ändern oder bestimmte IP-Adressen blockieren.

Die Ajax-Proxy-Datei `proxy-config.xml` befindet sich an einer der folgenden Positionen:

- Wenn Sie die Business Space-Umgebung verwenden, die mit Ihrem BPM-Produkt ausgeliefert wurde: `profilstammverzeichnis/BusinessSpace/knotenname/servername/mm.runtime.prof/config/proxy-config.xml`.

Hilfeinformationen zu Problemen mit dem Ajax-Proxy finden Sie in den technischen Hinweisen zu IBM Mashups unter <http://www-01.ibm.com/support/search.wss?tc=SSWP9P>.

**Wichtig:** Der Ajax-Proxy-Server ist so konfiguriert, dass er standardmäßig geschlossen ist, aber eine Standardrichtlinie aufweist, mit der auf alle Business Space-Endpunkte zugegriffen werden kann. Folgen Sie den unter Proxy-Richtlinien zum Business Space-Ajax-Proxy-Server hinzufügen angegebenen Schritten, um einen Zugriff auf zusätzliche URLs zu ermöglichen, und führen Sie die in IP-Adressen mithilfe des Business Space-Ajax-Proxy-Servers blockieren angegebenen Schritte aus, um den Zugriff auf bestimmte IP-Adressen einzuschränken.

1. Ändern Sie die Datei `proxy-config.xml` nach Bedarf.

Wenn Sie zum Beispiel die Einstellung für die Zeitlimitüberschreitung für den Business Space-Ajax-Proxy ändern, müssen Sie den Wert von `proxy:value` für `socket-timeout` ändern.

2. Führen Sie den Befehl `updateBlobConfig` über den Scripting-Client 'wsadmin' aus und geben Sie dabei die folgenden Parameter an: **-serverName** und **-nodeName** für einen eigenständigen Server oder **-clusterName** für einen Cluster, **-propertyFileName** mit dem Wert des Pfads für die Datei `proxy-config.xml` und **-prefix** mit dem Wert `Mashups_`.

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updateBlobConfig('[-serverName servername -nodeName knotenname
-propertyFileName "profilstammverzeichnis/BusinessSpace/node_name/
server_name/mm.runtime.prof/config/proxy-config.xml" -prefix
"Mashups_"]')
```

```
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```

$AdminTask updateBlobConfig {-serverName servername -nodeName knotename
-propertyFileName "profilstammverzeichnis/BusinessSpace/node_name/
server_name/mm.runtime.prof/config/proxy-config.xml" -prefix "Mashups_"}
$AdminConfig save

```

### Proxy-Richtlinien zum Ajax-Proxy von Business Space hinzufügen:

Fügen Sie zusätzliche Proxy-Richtlinien zur Datei proxy-config.xml hinzu, damit Business Space in einer dezentralen Umgebung ordnungsgemäß arbeitet.

Der Business Space Ajax-Proxy-Server enthält vordefinierte Richtlinien für bestimmte IBM URLs, ist aber nicht für alle URLs offen. Wenn Sie Ressourcen aus fernen Sites in Business Space nutzen, müssen Sie der Datei proxy-config.xml neue Richtlinien hinzufügen. Dies geschieht auf der Basis der Formatierung einer der vordefinierten Richtlinien, zum Beispiel `<proxy:policy url="http://www-03.ibm.com/*" acf="none" basic-auth-support="true">`, damit von fernen Sites bereitgestellter Inhalt in den Widgets 'Web Feed' und 'Google Gadgets' ordnungsgemäß dargestellt wird.

Wenn Sie mit einer älteren Version von Business Space gearbeitet haben und möchten, dass der Ajax-Proxy-Server weiterhin für alle URLs offen bleibt (wie bei der früheren Version), müssen Sie `<proxy:policy url="endpoint://*" acf="none" basic-auth-support="true">` in `<proxy:policy url="*" acf="none" basic-auth-support="true">` ändern.

1. Öffnen Sie die Datei proxy-config.xml. Die Position der Ajax-Proxy-Server-Datei können Sie dem Abschnitt „Business Space-Ajax-Proxy konfigurieren“ auf Seite 327 entnehmen.
2. Um den Ajax-Proxy-Server so zu beschränken, dass er nur auf bestimmte Endpunkte Zugriff gestattet, müssen Sie sicherstellen, dass die Datei proxy-config.xml die Vorgabe `<proxy:policy url="endpoint://*" acf="none" basic-auth-support="true">` anstelle von `<proxy:policy url="*" acf="none" basic-auth-support="true">` enthält.
3. Richtlinien für fernen Inhalt hinzufügen.

Die folgenden vordefinierten Richtlinien ermöglichen den Zugriff auf Web-Feeds über bestimmte ferne Sites, damit diese ordnungsgemäß im Widget für Web-Feeds funktionieren.

```

<proxy:policy url="http://www.ibm.com/*" acf="none" basic-auth-support="true">
<proxy:actions>
<proxy:method>GET</proxy:method>
</proxy:actions>
</proxy:policy>

```

```

<proxy:policy url="http://www-03.ibm.com/*" acf="none" basic-auth-support="true">
<proxy:actions>
<proxy:method>GET</proxy:method>
</proxy:actions>
</proxy:policy>

```

```

<proxy:policy url="http://www.redbooks.ibm.com/*" acf="none" basic-auth-support="true">
<proxy:actions>
<proxy:method>GET</proxy:method>
</proxy:actions>
</proxy:policy>

```

Damit Sie auf zusätzliche Web-Feeds, Google Gadgets oder sonstigen fernen Inhalt zugreifen können, müssen Sie, wie im folgenden Beispiel beschrieben, eine Richtlinie hinzufügen:



```

<proxy:policy url="http://your_URL" acf="none" basic-auth-support="true">
<proxy:actions>
<proxy:method>GET</proxy:method>
</proxy:actions>
</proxy:policy>

```

- Schließen Sie die Ajax-Proxy-Server-Konfiguration den Anforderungen Ihrer Umgebung entsprechend ab. Weitere Informationen enthält der Abschnitt „Business Space-Ajax-Proxy konfigurieren“ auf Seite 327.

#### **Einstellung für die Zeitlimitüberschreitung für den Business Space-Ajax-Proxy ändern:**

Business Space verwendet eine Proxy-Serverkomponente, um eine Verbindung zu Ihren REST-Services herzustellen. Falls die REST-Services nicht reagieren, müssen Sie die Einstellungen für das Verbindungszeitlimit zwischen Business Space und Ihren REST-Services aktualisieren, je nachdem, wie die Leistung auf den Servern für die REST-Services ist.

Falls die REST-Serviceverbindungen das Zeitlimit überschreiten, aktualisieren Sie die folgenden Einstellungen:

Wenn Sie die Business Space-Umgebung verwenden, die mit Ihrem BPM-Produkt ausgeliefert wurde, liegt der Standardwert für die Socket-Zeitlimitüberschreitung (socket-timeout) bei 30 Sekunden. Ändern Sie ihn in einen zu Ihrer Situation passenden Wert.

Wenn Sie Business Space mit WebSphere Portal verwenden, liegt der Standardwert für die Socket-Zeitlimitüberschreitung (socket-timeout) bei 10 Sekunden. Ändern Sie ihn in einen zu Ihrer Situation passenden Wert (30 Sekunden, wenn Sie die IBM Business Process Manager -Verwaltungswidgets verwenden).

- Öffnen Sie die Datei proxy-config.xml. Die Position der Ajax-Proxy-Datei können Sie dem Abschnitt „Business Space-Ajax-Proxy konfigurieren“ auf Seite 327 entnehmen.
- Ändern Sie den Wert proxy:value für socket-timeout. Die Zeit wird in Millisekunden angegeben.

```

<proxy:meta-data>
  <proxy:name>socket-timeout</proxy:name>
  <proxy:value>30000</proxy:value>
</proxy:meta-data>

```

- Schließen Sie die Ajax-Proxy-Konfiguration den Anforderungen Ihrer Umgebung entsprechend ab. Weitere Informationen finden Sie unter „Business Space-Ajax-Proxy konfigurieren“ auf Seite 327.

#### **IP-Adressen mit dem Business Space-Ajax-Proxy-Server blockieren:**

Der Ajax-Proxy-Server leitet Anforderungen von Widgets an Ihre Produkt- und Zielsever weiter, wenn die Server remote auf den Business Space-Server zugreifen. Der Ajax-Proxy-Server-Server ist so konfiguriert, dass er standardmäßig geschlossen ist, jedoch eine Standardrichtlinie bereitstellt, mit der auf alle Business Space-Endpunkte zugegriffen werden kann. Sie können den Ajax-Proxy so konfigurieren, dass der Zugriff auf bestimmte IP-Adressen eingeschränkt wird.

**Wichtig:** Der Ajax-Proxy-Server-Server ist so konfiguriert, dass er standardmäßig geschlossen ist, aber eine Standardrichtlinie aufweist, mit der auf alle Business Space-Endpunkte zugegriffen werden kann. Folgen Sie den unter Proxy-Richtlinien zum Business Space-Ajax-Proxy-Server hinzufügen angegebenen Schritten, um ei-

nen Zugriff auf zusätzliche URLs zu ermöglichen, und führen Sie die unten angegebenen Schritte aus, um den Zugriff auf bestimmte IP-Adressen einzuschränken.

Wenn Sie den Zugriff auf bestimmte IP-Adressen beschränken möchten, können Sie den Ajax-Proxy-Server so konfigurieren, dass IP-Adressen gefiltert werden und der Zugriff auf diese Adressen erlaubt oder verweigert wird. Sie können Blacklist- oder Whitelist-Regeln in der Datei `proxy-config.xml` definieren.

1. Öffnen Sie die Datei `proxy-config.xml`. Die Position der Ajax-Proxy-Server-Datei können Sie dem Abschnitt „Business Space-Ajax-Proxy konfigurieren“ auf Seite 327 entnehmen.
2. Fügen Sie Filterregeln hinzu, um den Zugriff zu ermöglichen oder zu verweigern.

Wenn Sie eine Blacklist-Regel für eine bestimmte IP-Adresse oder für eine Gruppe von Adressen definieren möchten, verwenden Sie ein Element `proxy:deny`. Zum Definieren einer Whitelist-Regel für eine bestimmte IP-Adresse oder für eine Gruppe von Adressen verwenden Sie hingegen ein Element `proxy:allow`. Die Filterregeln werden in der angegebenen Reihenfolge angewendet, wobei die letzte anwendbare Filterregel Vorrang vor vorherigen Filterregeln hat.

Fügen Sie die Information `<proxy:ipfilter>` zu den Proxy-Regeln der Datei `proxy-config.xml` hinzu (nach der Angabe der Proxy-Richtlinien und vor den `</Proxy-Regeln>`).

```
<proxy:ipfilter>
<proxy:deny>9.6.0.0/255.255.0.0</proxy:deny>
<proxy:allow>9.6.1.0/255.255.255.0</proxy:allow>
<proxy:deny>9.6.1.4</proxy:deny>
</proxy:ipfilter>
```

In diesem Beispiel führt der IP-Filter die folgenden Filter aus:

- Blockieren aller IP-Adressen 9.6.\*.\*
- Zulassen aller Adressen 9.6.1.\*, aber Blockieren der IP-Adresse 9.6.1.4

In diesem Fall würde der Proxy keinen Zugriff auf die IP-Adresse 9.6.2.5 oder 9.6.120.7 zulassen und folgende Nachricht ausgeben: `BMWPX0018E: Die IP-Adresse des Zielhosts ist gemäß einer Regel nicht zulässig.`

Der Zugriff auf 9.6.1.5 oder 9.6.1.120 ist zulässig, aber der Zugriff 9.6.1.4 wird verweigert.

Beim Hinzufügen neuer Filterregeln können Sie diese auf vielfältige Weise kombinieren, aber sie werden vom Proxy immer in Folge bearbeitet. Das bedeutet, dass die letzte Abgleichsregel immer in Kraft tritt, unabhängig von zuvor aufgeführten zulassenden oder zurückweisenden Regeln.

3. Schließen Sie die Ajax-Proxy-Server-Konfiguration den Anforderungen Ihrer Umgebung entsprechend ab. Weitere Informationen finden Sie unter „Business Space-Ajax-Proxy konfigurieren“ auf Seite 327.

### **Business Space migrieren (nach Produktmigration)**

Nach der Migration Ihres Produkts auf V8.0, müssen Sie einige zusätzliche Tasks für Business Space ausführen, bevor Sie Ihre Server oder Cluster starten.

Bevor Sie mit dieser Task beginnen, müssen Sie Ihren Produktserver oder -cluster migriert und geprüft haben, ob die Migration erfolgreich war.

Sie müssen außerdem die Datenbank migriert haben, die Sie für Business Space verwenden. Befolgen Sie für die Migration der Datenbanken und Daten die Anweisungen, die sich auf Ihr Produkt beziehen.

Falls Sie die Migration von einer früheren Version Ihres Produkts ausführen und wenn Business Space konfiguriert ist, müssen Sie nach der Migration die folgenden Schritte ausführen, bevor Sie Business Space verwenden können.

1. Wenn Sie in einem früheren Release mit benutzerdefinierten Widgets gearbeitet haben, müssen Sie die folgenden manuellen Schritte ausführen, um die Widgets für Business Space V8.0 betriebsbereit zu machen. Weitere Informationen finden Sie unter Benutzerdefinierte Widgets migrieren.

**Tipp:** Die V7.0-Datenmigration unterstützt Sie bei der Migration des Widgetkatalogs und der Endpunkte Ihrer benutzerdefinierten Widgets, sodass Sie diese nicht manuell erneut migrieren müssen.

2. Wenn Sie im Vorgängerrelease eine Umgebung hatten, in der Business Space in einer anderen Zelle als die REST-Services ausgeführt wurde oder in der Widgets in anderen Zellen als Business Space ausgeführt wurden, müssen Sie die Endpunktdateien aktualisieren. Weitere Informationen finden Sie unter Business Space-Widgets für zellenübergreifende Umgebungen aktivieren.
3. Wenn Sie im Vorgängerrelease IBM Forms Server in Ihrer Umgebung mit Widgets für die Benutzertaskverwaltung verwendet haben, führen Sie die folgenden Schritte durch, um den Einsatz von Business Space mit IBM Forms Server V4.0 und der Webform Server-Komponente zu ermöglichen.
  - a. Installieren Sie IBM Forms Server V4.0.
  - b. Aktualisieren Sie in der Administrationskonsole Ihres Produkts die folgenden Umgebungsvariablen:
    - Ändern Sie die API-Referenzen 76 in 80, z. B.:  
`${LFS_API_DIR};${LFS_API_DIR}/80/system;`
    - Ändern Sie den Wert der Variable LFS\_DIR in den Pfad der IBM Forms Server-Installation, z. B.: `c:\Programme\IBM Forms Server\4.0\WebformServer.`

Weitere Informationen finden Sie unter IBM Forms Server für Widgets für die Benutzertaskverwaltung in Business Space konfigurieren.

4. Wenn Sie Spaces oder Vorlagen aus Ihrer vorherigen Business Space-Umgebung exportiert haben, importieren Sie sie in Business Space V8.0 um sie weiter verwenden zu können. Weitere Informationen finden Sie unter Spaces importieren und Vorlagen importieren.

**Tipp:** Wenn Sie von Version 6.x migriert haben, müssen Sie Vorlagen zunächst als Spaces in Space Manager importieren und die importierten Spaces dann in Vorlagen konvertieren, indem Sie auf **Aktionen > Als Vorlage speichern** klicken.

Nach Ausführung dieser Migrationsprozeduren können Sie Business Space V8.0 verwenden.

**Tipp:** Falls Sie zuvor Business Space V6.2 verwendet haben, müssen Sie den Browser-Cache löschen, bevor Sie Business Space V8.0 verwenden können. Dies verhindert eine unbeabsichtigte weitere Verwendung von Code und Bildern aus Business Space V6.2.

## **Business Space für die Verwendung mit Mashup Center konfigurieren**

Wenn Sie Business Space für die Verwendung mit IBM Mashup Center konfigurieren, können Business Space-Benutzer Vorlagen und Seiten im Mashup Center-Katalog publizieren, Mashup Center-Vorlagen zum Erstellen von Spaces verwenden und einzelne Seiten aus Mashup Center in Business Space importieren.

Um Business Space zusammen mit Mashup Center verwenden zu können, müssen Sie eine gültige Lizenz für Mashup Center besitzen. Business Space kann nur mit Widgets arbeiten, die in Business Space registriert sind, oder mit Widgets, die in Mashup Center publiziert wurden.

Wenn Mashup Center (einschließlich IBM InfoSphere MashupHub) nicht auf demselben Anwendungsserver wie Business Space ausgeführt wird, aktivieren Sie die Single-Sign-on-Funktionalität zwischen den beiden Anwendungsservern. Hierfür muss Ihre Umgebung ein eingebundenes Repository für Ihre Benutzerregistry verwenden. Weitere Informationen finden Sie unter LTPA-Schlüssel importieren und LTPA-Schlüssel exportieren im Information Center zu WebSphere Application Server. Richten Sie außerdem die SSL-Zertifikate ein. Weitere Informationen finden Sie unter Sichere Kommunikation mit Secure Sockets Layer (SSL) im Information Center zu WebSphere Application Server.

Damit Business Space zusammen mit Mashup Center verwendet werden kann, müssen Sie eine der folgenden Prozeduren für einen eigenständigen Server bzw. eine Clusterumgebung ausführen.

- Bei einem eigenständigen Server führen Sie folgende Schritte aus:
  1. Ändern Sie die Eigenschaft `com.ibm.mashups.hub.url` in der Konfigurationsdatei `profilstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties` und geben Sie dafür die URL für die MashupHub-Komponente von Mashup Center an (`protokoll://host:port/mashuphub`).
  2. Führen Sie den Befehl **updatePropertyConfig** in der 'wsadmin'-Umgebung des Profils aus:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig(['-serverName servername -nodeName knotenname -propertyFileName "profile_root\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

**Wichtig:** Für Windows muss der Wert für den Parameter **propertyFileName** der vollständige Pfad zu der Datei sein, und alle Backslashes müssen doppelt angegeben werden. Beispiel: `AdminTask.updatePropertyConfig(['-serverName servername -nodeName knotenname -propertyFileName "profilstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')`.

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-serverName servername -nodeName knotenname -propertyFileName "profilstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

3. Öffnen Sie die Konfigurationsdatei `profilstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\Endpoints.properties` und ändern Sie die Eigenschaft `oob.Widget.url` in die URL für Mashup Center (`protokoll://host:port/`).
4. Führen Sie den Befehl **updatePropertyConfig** in der 'wsadmin'-Umgebung des Profils aus:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-serverName servername -nodeName
knotenname -propertyFileName "profilstammverzeichnis\BusinessSpace\
knotenname\servername\mm.runtime.prof\config\Endpoints.properties"
-prefix "Mashups_"]')
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-serverName servername -nodeName kno-
tename -propertyFileName "profilstammverzeichnis\BusinessSpace\
knotenname\servername\mm.runtime.prof\config\Endpoints.properties"
-prefix "Mashups_" }
$AdminConfig save
```

5. Starten Sie den Server erneut.

- Bei einem Cluster führen Sie folgende Schritte aus:

1. Ändern Sie die Eigenschaft `com.ibm.mashups.hub.url` in der Konfigurationsdatei `deployment_manager-profilstammverzeichnis\BusinessSpace\clustername\mm.runtime.prof\config\ConfigService.properties` und geben Sie dafür die URL für die Mashup Center MashupHub-Komponente an (`protokoll://host:port/mashuphub`).

2. Führen Sie vom Deployment Manager aus den Befehl **updatePropertyConfig** in der wsadmin-Umgebung des Profils aus:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-clusterName clustername
-propertyFileName "deployment_manager-profilstammverzeichnis\
BusinessSpace\clustername\mm.runtime.prof\config\
ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-clusterName clustername
-propertyFileName "deployment_manager-profilstammverzeichnis\
BusinessSpace\clustername\mm.runtime.prof\config\
ConfigService.properties" -prefix "Mashups_" }
$AdminConfig save
```

3. Öffnen Sie die Konfigurationsdatei `profilstammverzeichnis\BusinessSpace\knotenname\servername\mm.runtime.prof\config\Endpoints.properties` und ändern Sie die Eigenschaft `oob.Widget.url` in die URL für Mashup Center (`protokoll://host:port/`).

4. Führen Sie vom Deployment Manager aus den Befehl **updatePropertyConfig** in der wsadmin-Umgebung des Profils aus:

Im folgenden Beispiel wird Jython verwendet:

```
AdminTask.updatePropertyConfig('[-clusterName clustername
-propertyFileName "deployment_manager-profilstammverzeichnis\
BusinessSpace\clustername\mm.runtime.prof\config\Endpoints.properties"
-prefix "Mashups_"]')
AdminConfig.save()
```

Im folgenden Beispiel wird Jacl verwendet:

```
$AdminTask updatePropertyConfig {-clusterName clustername
-propertyFileName "deployment_manager-profilstammverzeichnis\
BusinessSpace\clustername\mm.runtime.prof\config\Endpoints.properties"
-prefix "Mashups_" }
$AdminConfig save
```

5. Führen Sie einen Neustart des Deployment Managers aus.

## Widgets für den kombinierten Einsatz mit WebSphere Portal konfigurieren

Wenn Ihr Team IBM WebSphere Portal verwendet, können Sie Ihre Business Space-Widgets für den Einsatz in der WebSphere Portal-Umgebung konfigurieren.

Bevor Sie Widgets für die Verwendung mit WebSphere Portal konfigurieren, müssen Sie die folgenden Tasks ausführen:

- Installieren Sie WebSphere Portal V7.0.0.2 mit kumulativem Fix 12 oder höher.
- Stellen Sie sicher, dass Sie das Thema von WebSphere Portal V7.0.0.2 installiert haben. Weitere Informationen finden Sie im Abschnitt zur Themaaktivierung in der WebSphere Portal-Dokumentation.
- Stellen Sie sicher, dass Sie das vollständige Profil auf die Seiten, die Ihre Widgets enthalten, oder auf das gesamte Thema anwenden. Informationen finden Sie in den folgenden Abschnitten der WebSphere Portal-Dokumentation: Profilüberschreibung für eine Seite festlegen und Standardprofil für ein Thema ändern.
- Installieren und konfigurieren Sie das IBM Produkt, in dem Business Space V8.0 enthalten ist.
- Konfigurieren Sie Ihre REST-Services (Representational State Transfer Service), damit Widgets zur Laufzeit darauf zugreifen können. Weitere Informationen finden Sie unter „REST-Services konfigurieren“ auf Seite 243.
- Konfigurieren Sie SSL und SSO. Weitere Informationen finden Sie unter „SSO und SSL für Widgets in WebSphere Portal konfigurieren“ auf Seite 339.
- Führen Sie spezielle Konfigurationsschritte für die Widgets aus (sofern erforderlich).
- Wenn Sie Widgets für die Benutzertaskverwaltung in einer Clusterumgebung verwenden, stellen Sie sicher, dass Sie DOJO-Formulare auf demselben Knoten wie die Widgets installieren.

Beim Konfigurieren von Business Space-Widgets für WebSphere Portal müssen die folgenden Punkte beachtet werden:

- Installieren Sie Ihr Produkt nicht in einem WebSphere Portal-Profil.

**Einschränkung:** Nicht alle Produktwidgets können unter WebSphere Portal ausgeführt werden. Prüfen Sie, welche Umgebungen von Ihrem Produkt unterstützt werden.

1. Erstellen Sie Endpunktreferenzen auf dem WebSphere Portal-Anwendungsserver. Business Space und produktspezifische Endpunktreferenzeinträge müssen erstellt werden, damit Business Space in der WebSphere Portal-Umgebung richtig ausgeführt wird. Endpunkte müssen auf dem WebSphere Portal-Server definiert werden, aber sie werden remote durch Ausführung des Befehls **updateEndpointBindingsOnPortal** auf Ihrem Produktserver erstellt.
  - a. Starten Sie den WebSphere Portal-Server und Ihren Produktserver.
  - b. Kopieren Sie die Serviceendpunktdateien von Business Space und Ihrem Produkt in ein temporäres Verzeichnis auf Ihrer Produktmaschine, z. B. `c:/tmp/endpoints/`.

Die Serviceendpunktdateien befinden sich auf Ihrem Produktserver in den folgenden Verzeichnissen:

- `profilstammverzeichnis/BusinessSpace/knotenname/servername/mm.runtime.prof/endpoints/`



- *installationsstammverzeichnis/BusinessSpace/registryData/produktname/endpoints*

Einige Endpunktdateien sind unter Umständen doppelt vorhanden. Kopieren Sie nur die Endpunktdateien, für die Sie Einträge erstellen müssen. Dateien, die zuvor mit dem Befehl **updateEndpointBindingsOnPortal** verarbeitet wurden, müssen nicht kopiert werden. Die folgende Liste enthält IBM Geschäftsprozessmanagementbeispiele von Serviceendpunktdateien und Widgetendpunktdateien:

- IBM Business Monitor: *monitorEndpoints.xml* und *monitorWidget.xml*
  - IBM Business Monitor mit IBM Cognos Business Intelligence: *cognosEndpoints.xml* und *cognosWidget.xml*
  - WebSphere Enterprise Service Bus: *wesbWidgetEndpoints.xml* (für Widgets 'Mediationsrichtlinienverwaltung', 'Service-Browser' und 'Proxy-Gateway'), *bpmAdministrationEndpoints.xml* und *BPMAdministrationWidgetEndpoints.xml* (für Widgets 'Verwaltung')
  - IBM Business Process Manager: *wpsEndpoints.xml*, *bpmAdministrationEndpoints.xml* und *BPMAdministrationWidgetEndpoints.xml* (für Widgets 'Verwaltung'), *wesbWidgetEndpoints.xml* (für Widgets 'Mediationsrichtlinienverwaltung', 'Service-Browser' und 'Proxy-Gateway'), *HumanTaskManagementEndpoints.xml* für Business-Prozesse und Benutzer-tasks, *bspaceWFSEndpoints.xml* (für die Verwendung von Lotus Webform Server mit den Widgets 'Benutzertaskverwaltung').
  - Alle Produkte: *wsumEndpoint.xml* und *wsumWidget.xml* (für Benutzerzugehörigkeit)
- c. Bearbeiten Sie in einer verteilten Umgebung die Serviceendpunktdateien so, dass sie auf die richtigen URLs verweisen.

Da die Endpunkte bei dem Anwendungsserver registriert sind, auf dem das Hosting des WebSphere Portal-Servers erfolgt, müssen alle Endpunkte auf den fernen Business Space-Server verweisen. Die Endpunkte müssen den vollständig qualifizierten Namen oder die IP-Adresse des fernen Hosts beinhalten, z. B.:

```
<tns:Endpoint>
  <tns:id>{com.ibm.bspace}bpaceCommonWidgetRootId</tns:id>
  <tns:type>{com.ibm.bspace}bpaceCommonWidgetRootId</tns:type>
  <tns:version>1.0.0.0</tns:version>
  <tns:url>http://<Business_Space_Host>:<port>/BusinessSpace/</tns:url>
  <tns:description>Position der allgemeinen Business Space-Widgets</tns:description>
</tns:Endpoint>
```

Konfigurieren Sie die Endpunkte nach Bedarf durch Bearbeitung der Serviceendpunktdateien. Jeder in der Datei enthaltene Endpunkt wird durch einen Block `<tns:Endpoint>` definiert. Identifizieren Sie den zu ändernden Block. Suchen Sie nach Kommentaren, die Ihnen einen Hinweis darauf geben, wo Sie die Bearbeitung vornehmen müssen, z. B.:

```
<!-- Befindet sich der REST-Service nicht lokal auf Ihrem Business Space-Server, aktualisiere -->
<tns:url>/rest/bpm/monitor/</tns:url>
```

**Tipp:** Wenn Sie vorhaben, bestimmte Endpunkte nicht zu aktivieren, können Sie diese aus der Datei entfernen, um Unklarheiten zu vermeiden.

Die durch einen Endpunkt identifizierte Position wird in `<tns:url>` angegeben. Dieser Wert ist ein Pfad in einem Webmodul, der als vollständige oder relative HTTP-URL angegeben wird. Standardmäßig wird eine relative URL angegeben. Ändern Sie diese Angabe in einen vollständigen URL-Pfad, z. B. `https://virtueller_host.com:virtueller_port/rest/bpm/htm` oder `http://`

host1:9445/WBPublishingDRAFT/. Das Protokoll, der Host und der Port geben an, wie der Zugriff auf das Webmodul des Produkts erfolgt.

Führen Sie die folgenden Arbeitsschritte aus, um die Portnummer für den Server zu suchen:

- Melden Sie sich bei der Administrationskonsole an.
- Klicken Sie auf **Server > Servertypen > WebSphere-Anwendungsserver**.
- Klicken Sie auf den Server, dessen Portnummer gesucht werden soll, und erweitern Sie dann die Anzeige des Abschnitts für die Ports.

Alle Anwendungen verwenden denselben Port, der im Parameter **wc\_defaulthost** (nicht gesicherter Host) oder im Parameter **wc\_defaulthost\_secure** (gesicherter Host) angegeben ist.

**Wichtig:** Wenn Sie einen HTTP-Server verwenden, um auf Ihre Webmodule für den Lastausgleich zuzugreifen, verwenden Sie den Hostnamen und die Porteinstellungen des HTTP-Servers.

- d. Öffnen Sie eine wsadmin-Sitzung auf Ihrem Produktserver. Führen Sie die Datei wsadmin.bat oder wsadmin.sh im Verzeichnis *profilstammverzeichnis/bin/* aus. Die wsadmin-Sitzung stellt eine Verbindung zu der Java Virtual Machine des lokalen Produktanwendungsservers her.
  - e. Führen Sie in der wsadmin-Sitzung den Befehl **updateEndpointBindingsOnPortal** aus. (In einer Network Deployment-Umgebung ist der Befehl von einem Deployment Manager aus auszuführen.)
    - Jython-Beispiel:

```
AdminTask.updateEndpointBindingsOnPortal(['[-nodeName  
Portal-knotenname -serverName WebSphere_Portal  
-endpointBindingDirectoryName verzeichnis_mit_endpunktdateien -host  
IP_oder_hostname_des_Portal-servers -port Portal-SOAP-  
standardport_10025 -user Portal-administrator-ID -password  
Portal-administatorkennwort]'])
```
    - Jacl-Beispiel:

```
$AdminTask updateEndpointBindingsOnPortal {-nodeName  
Portal-knotenname -serverName WebSphere_Portal  
-endpointBindingDirectoryName verzeichnis_mit_endpunktdateien -host  
IP_oder_hostname_des_Portal-servers -port Portal-SOAP-  
standardport_10025 -user Portal-administrator-ID -password  
Portal-administratorkennwort}
```
  - f. Führen Sie einen Neustart des WebSphere Portal-Servers aus.
  - g. Prüfen Sie in der WebSphere Portal-Administrationskonsole die Endpunkte, indem Sie zu dem Ressourcenumgebungsprovider mit dem Namen **WP Mashup Endpoints** navigieren. Klicken Sie auf **Ressourcen > Ressourcenumgebung > Ressourcenumgebungsprovider > providername > Angepasste Eigenschaften**.
2. Konfigurieren Sie den Ajax-Proxy-Server auf dem WebSphere Portal-Server. Um Remote URLs den Zugriff vom WebSphere Portal-Server auf Ihren Produktserver zu ermöglichen, müssen Sie den Ajax-Proxy-Server konfigurieren.
    - a. Aktualisieren Sie Ihre vorhandene Datei proxy-config.xml mit dem Mustercodeausschnitt für die Proxy-Richtlinie, der in „Erforderliche Einträge für die Datei proxy-config.xml zur Konfiguration von Widgets für den kombinierten Einsatz mit WebSphere Portal“ auf Seite 341 gezeigt wird.
    - b. Führen Sie das Script **checkin-wp-proxy-config** aus.

In einer Clusterumgebung müssen Sie das Script auf dem primären Knoten ausführen.

```
ConfigEngine.[bat|sh] checkin-wp-proxy-config
-DProxyConfigFileName=verzeichnispfad/temporäre_proxy-datei.name
-DWasPassword=kennwort_des_anwendungsservers -DWasUserid=benutzer-
ID_des_anwendungsservers -DPortalAdminId=WebSphere_Portal-
administrator-ID -DPortalAdminPwd=WebSphere_Portal-
administratorkennwort. Dabei ist verzeichnispfad/temporäre_proxy-datei.name
der vollständige Pfad Ihrer geänderten Datei wp.proxy.config.xml.
```

Weitere Informationen zur Proxy-Konfiguration finden Sie in der WebSphere Portal-Dokumentation unter [http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Global\\_proxy\\_configuration\\_wp7](http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Global_proxy_configuration_wp7).

c. Führen Sie von der Administrationskonsole einen Neustart der Anwendung **AJAX Proxy Configuration** aus.

3. Registrieren Sie die Business Space-Widgets unter WebSphere Portal.

Business Space-Widgets werden bei WebSphere Portal mittels eines Massenimports als iWidgets registriert; dies geschieht unter Verwendung der WebSphere Portal-spezifischen Widgetkatalogdatei zusammen mit Ihrem Produkt. Die XML-Katalogdatei ist im Stammverzeichnis der Webarchivdatei (WAR) des Produkts enthalten. Jedes Produkt hat ein eigenes Kontextstammverzeichnis.

Es gibt zwei Arten von Widgets: allgemeine Widgets und produktspezifische Widgets.

Das Kontextstammverzeichnis für die gemeinsamen Business Space-Widgets ist */BusinessSpace* und die Katalogdatei ist *catalog\_commonWidgets\_portal.xml*. Beispiel: Geben Sie die URL für die XML-Katalogdatei für die gemeinsamen Business Space-Widgets wie folgt an: [http://localhost:9080/BusinessSpace/catalog\\_commonWidgets\\_portal.xml](http://localhost:9080/BusinessSpace/catalog_commonWidgets_portal.xml).

Die folgenden URLs sind Beispiele für BPM-Produkte:

- IBM Business Monitor: [http://Business\\_Space\\_hosting-monitor:port/BusinessDashboard/catalog.xml](http://Business_Space_hosting-monitor:port/BusinessDashboard/catalog.xml)
- IBM Business Monitor mit IBM Cognos Business Intelligence: [http://Business\\_Space-hosting-Monitor:port/CognosWidgets/catalog.xml](http://Business_Space-hosting-Monitor:port/CognosWidgets/catalog.xml)
- Widgets für die Benutzertaskverwaltung: [http://Business\\_Space-hosting-Business\\_Process\\_Manager:port/HumanTaskManagementWidgets/portal\\_catalog.xml](http://Business_Space-hosting-Business_Process_Manager:port/HumanTaskManagementWidgets/portal_catalog.xml)
- Widgets für die Verwaltung:
  - [http://Business\\_Space\\_hosting\\_Business\\_Process\\_Manager:port/BSpaceWidgetsHM/hmCatalog.xml](http://Business_Space_hosting_Business_Process_Manager:port/BSpaceWidgetsHM/hmCatalog.xml)
  - [http://Business\\_Space\\_hosting\\_Business\\_Process\\_Manager:port/PolymorphicWidget/polymorphicCatalog.xml](http://Business_Space_hosting_Business_Process_Manager:port/PolymorphicWidget/polymorphicCatalog.xml)
  - [http://Business\\_Space\\_hosting\\_Business\\_Process\\_Manager:port/scaWidget/scaCatalog.xml](http://Business_Space_hosting_Business_Process_Manager:port/scaWidget/scaCatalog.xml)
  - [http://Business\\_Space\\_hosting\\_Business\\_Process\\_Manager:port/SecurityManagerWidgets/smCatalog.xml](http://Business_Space_hosting_Business_Process_Manager:port/SecurityManagerWidgets/smCatalog.xml)
  - [http://Business\\_Space\\_hosting\\_Business\\_Process\\_Manager:port/StoreAndForward/sfCatalog.xml](http://Business_Space_hosting_Business_Process_Manager:port/StoreAndForward/sfCatalog.xml)

—  
`http://Business_Space_hosting_Business_Process_Manager:port/  
ServiceMonitorGraphWidget/smGraphCatalog.xml`  
—

`http://Business_Space_hosting_Business_Process_Manager:port/  
BSpaceWidgetsBCM/bcCatalog.xml`

- a. Führen Sie den folgenden Befehl von `wp-profil\ConfigEngine` aus, um iWidgets unter Verwendung der catalog-XML-Datei Ihres Produkts zu registrieren:

```
ConfigEngine.[bat|sh] register-iwidget-definition  
-DIWidgetCatalog=URL_zu_XML-katalogdatei -DWasPassword=kennwort  
-DWasUserid=ID -DPortalAdminId=ID -DPortalAdminPwd=kennwort  
-DRegistrationAspects=catalogTitlesOverule,considerWidgetParam,considerUniqueName
```

Beispiel für IBM Business Monitor:

```
ConfigEngine.bat register-iwidget-definition -DIWidgetCatalog=http://  
localhost:9080/BusinessDashboard/catalog.xml -DWasPassword=admin  
-DWasUserid=admin -DPortalAdminId=admin -DPortalAdminPwd=admin  
-DRegistrationAspects=catalogTitlesOverule,considerWidgetParam,considerUniqueName
```

- b. Um zu prüfen, ob der Befehl richtig ausgeführt wurde, suchen Sie nach `Return Value:0`. Weitere Informationen zu optionalen Befehlen finden Sie in der WebSphere Portal-Dokumentation unter [http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Task\\_registeriwidgetdefinition\\_wp7](http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Task_registeriwidgetdefinition_wp7).

Wenn Sie Business Space für den kombinierten Einsatz mit WebSphere Portal eingerichtet haben, führen Sie folgende Tasks aus:

- Wenn Sie IBM Business Monitor mit IBM Cognos Business Intelligence verwenden, müssen Sie den Abschnitt `ProxyServlet_Servlet` in der Datei `web.xml` aktualisieren. Weitere Informationen finden Sie in der Dokumentation zu IBM Business Monitor.
- Um bestimmte Business Space iWidgets zu suchen und einer WebSphere Portal-Seite hinzuzufügen und um die Arbeit in der WebSphere Portal-Umgebung aufzunehmen, melden Sie sich beim WebSphere Portal-Server an und klicken Sie auf **Aktionen > Seite bearbeiten**. Die Business Space-Widgets sind nur in der Kategorie **ALLE** sichtbar. Damit Sie Ihre Widgets finden, wählen Sie **ALLE** als Kategorie aus und den Namen des Widgets, das Sie hinzufügen möchten. Klicken Sie anschließend auf die Schaltfläche **Suchen**.
- Um den Ereignisaustausch zwischen iWidgets und nativen Portlets auf derselben Seite in WebSphere Portal zu aktivieren und um das Festhalten einzelner Navigationsstadien von Widgets nach Seitenwechseln zu aktivieren, konfigurieren Sie die Seiten mit Ihren Business Space-Widgets so, dass sie clientseitige Aggregation verwenden. Weitere Informationen dazu finden Sie in der Dokumentation zu WebSphere Portal.
- Um sicherzustellen, dass alle möglichen Ereignisse Ihrer Widgets angezeigt werden, wählen Sie, während Sie die Verbindungen der Widgets konfigurieren, **Semantiktyp oder Nutzdattentyp beim Abgleich von Quellen und Zielen berücksichtigen** als Abgleichungsmodus aus. Zum Ändern des Abgleichungsmodus öffnen Sie die Verbindungseditor und klicken auf **Einstellungen**. Anschließend wählen Sie **Semantiktyp oder Nutzdattentyp beim Abgleich von Quellen und Zielen berücksichtigen** aus und klicken auf **Fertig**.
- Stellen Sie sicher, dass die mit Ihrem Produkt mitgelieferten Widgets vernetzt werden, damit sie miteinander funktionieren. Konsultieren Sie hierzu die Produktdokumentation für Ihre Widget-Ereignisse. Für IBM Business Monitor siehe beispielsweise Widget-Ereignisse.

- Zum Anzeigen der Titel Ihrer Widgets müssen Sie als Thema **Portal 7.0.0.2 - Standard** festlegen. Standardmäßig werden Portlet-Titel in WebSphere Portal im Anzeigemodus nicht angezeigt. Möglicherweise werden daher einige der Wid- getmenüs nicht angezeigt. Wenn Sie als Thema **Portal 7.0.0.2 - Standard** festle- gen wollen, klicken Sie in der WebSphere Portal-Administrationskonsole auf **Ad- ministration > Manage Pages** und wählen für Ihre Seite die Optionen **Edit page layout > AppearancePortal 7.0.0.2 - Standard** aus. Anschließend werden die Portlet-Titel im Anzeigemodus angezeigt.

### SSO und SSL für Widgets in WebSphere Portal konfigurieren:

Damit Ihre Produktwidgets in WebSphere Portal verwendet werden können, müs- sen Sie zwischen WebSphere Portal und Ihrem Produkt, das Business Space-Wid- gets enthält, Single Sign-on (SSO) einrichten und Sie müssen die SSL-Zertifikate (Secure Sockets Layer) so konfigurieren, dass sie zwischen WebSphere Portal und Ihrem Produkt, das Business Space-Widgets enthält, ausgetauscht werden.

Sie müssen SSO zwischen den Servern für WebSphere Portal und Ihrem Produkt, das Business Space-Widgets enthält, konfigurieren. Richten Sie außerdem SSL zwi- schen WebSphere Portal und Ihrem Produkt mit den Business Space-Widgets ein. Dies setzt voraus, dass die SSL-Unterzeichnerzertifikate zwischen den Servern aus- getauscht werden.

Der Benutzername und das Kennwort für die Anmeldung an der Administrations- konsole müssen für den WebSphere Portal-Server und Ihren Produktserver iden- tisch sein.

**Tipp:** Wenn Sie getrennte Zellen konfiguriert haben, stellen Sie sicher, dass die SSO-Richtlinien berücksichtigt wurden (dazugehört auch, dass die LTPA-Schlüssel synchronisiert sind, gemeinsam genutzte Benutzernamen/Realmnamen synchroni- siert sind und geeignete Zertifikate importiert wurden). Bei IBM Business Process Manager können sich eventuell auch mehrere Repositories im Realm befinden, was unter Umständen einen Fehler durch die Fehlzuordnung von Realms auslöst. Siehe hierzu Realm in Konfiguration für föderierte Repositories verwalten in der Doku- mentation für WebSphere Application Server.

1. Richten Sie SSO zwischen WebSphere Portal und Ihrem Produkt, das Business Space-Widgets enthält, ein.
  - a. Melden Sie sich an der Administrationskonsole des Deployment Manager Ihres Produkts an, das Business Space-Widgets enthält.
  - b. Führen Sie die Schritte aus, die unter Schlüssel importieren und exportieren im Information Center zu WebSphere Application Server beschrieben sind.
2. Richten Sie die SSL-Zertifikate so ein, dass sie zwischen den Servern von Web- Sphere Portal und Ihres Produkts, das Business Space-Widgets enthält, ausge- tauscht werden.

Stellen Sie sicher, dass die Unterzeichner in den entsprechenden Truststores für den WebSphere Portal-Server und Ihren Produktserver konfiguriert sind. Weite- re Informationen finden Sie unter Sichere Kommunikation mit Secure Sockets Layer (SSL) im Information Center zu WebSphere Application Server.

### Befehl 'updateEndpointBindingsOnPortal':

Mit dem Befehl **updateEndpointBindingsOnPortal** können Sie Endpunktreferenzen auf dem WebSphere Portal-Anwendungsserver erstellen, sodass Ihr Team die Wid- gets in Business Space unter WebSphere Portal verwenden kann.



Dieser Befehl erstellt Referenzen zu den REST-Endpunkten (REST = Representational State Transfer) auf dem WebSphere Portal-Anwendungsserver. Business Space und produktspezifische Endpunktreferenzeinträge müssen erstellt werden, damit Business Space in der WebSphere Portal-Umgebung richtig ausgeführt wird. Business Space-Widgets werden bei WebSphere Portal mittels eines Massenimports als iWidgets registriert; dies geschieht unter Verwendung der WebSphere Portal-spezifischen Widgetkatalogdatei zusammen mit Ihrem Produkt. Die XML-Katalogdatei ist im Stammverzeichnis der Webarchivdatei (WAR) des Produkts enthalten. Jedes Produkt hat ein eigenes Kontextstammverzeichnis. Dieser Befehl kann nur für den Ressourcenumgebungsprovider WP Mashup Endpoints erfolgreich ausgeführt werden.

Bevor Sie diesen Befehl ausführen, müssen Sie WebSphere Portal ab V7.0.0.1 installieren, Business Space und REST-Services für Ihr Produkt konfigurieren sowie SSL und SSO konfigurieren. Weitere Informationen finden Sie im Abschnitt Business Space unter WebSphere Portal konfigurieren.

Speichern Sie Ihre Änderungen an der Masterkonfiguration nach der Ausgabe des Befehls mit einem der folgenden Befehle:

- Jython:  
AdminConfig.save()
- Jacl:  
\$AdminConfig save

#### Erforderliche Parameter

**-serverName** *WebSphere\_Portal-servername*

Dieser Parameter gibt den Namen des Zielservers für die WebSphere Portal-Konfiguration an. Für die Konfiguration von Business Space auf einem Server muss ein **Servername** und ein **Knotenname** angegeben werden.

**-nodeName** *WebSphere\_Portal-knotenname*

Dieser Parameter gibt den Namen des Zielknotens für die WebSphere Portal-Konfiguration an. Für die Konfiguration von Business Space auf einem Server muss ein **Servername** und ein **Knotenname** angegeben werden.

**-clusterName** *WebSphere\_Portal-clustername*

Dieser Parameter gibt den Namen des Zielclusters für die WebSphere Portal-Konfiguration an. Für die Konfiguration von Business Space in einem Cluster muss nur ein **clusterName** angegeben werden. Geben Sie weder **serverName** noch **nodeName** an.

**-host** *IP\_oder\_hostname\_des\_Portal-servers*

Dieser Parameter gibt die IP-Adresse oder den Hostnamen für den fernen WebSphere Portal-Server an.

**-port** *Portal-SOAP-standardport\_10025*

Dieser Parameter gibt den Namen des SOAP-Ports für den fernen WebSphere Portal-Server an.

**-user** *Portal-administrator-ID*

Dieser Parameter gibt die Administrator-ID für den fernen WebSphere Portal-Server an.

**-password** *Portal-administratorkennwort*

Dieser Parameter gibt das Administratorkennwort für den fernen WebSphere Portal-Server an.



**-endpointBindingDirectoryName** *verzeichnis\_mit\_endpunktdateien*

Dieser Parameter gibt das Verzeichnis an, das die Endpunktdateien enthält. Stellen Sie sicher, dass das Verzeichnis keine anderen Dateien enthält.

### Beispiel

Das folgende Beispiel erstellt Endpunktreferenzen auf dem WebSphere Portal-Anwendungsserver für eine eigenständige Umgebung.

- Beispiel mit Jython:

```
AdminTask.updateEndpointBindingsOnPortal(['-nodeName Portal-knotenname  
-serverName WebSphere_Portal -endpointBindingDirectoryName  
verzeichnis_mit_endpunktdateien -host IP_oder_hostname_des_Portal-servers  
-port Portal-SOAP-standardport_10025 -user Portal-administrator-ID  
-password Portal-administatorkennwort']])
```

- Beispiel mit Jacl:

```
$AdminTask updateEndpointBindingsOnPortal {-nodeName Portal-knotenname  
-serverName WebSphere_Portal -endpointBindingDirectoryName  
verzeichnis_mit_endpunktdateien -host IP_oder_hostname_des_Portal-servers  
-port Portal-SOAP-standardport_10025 -user Portal-administrator-ID  
-password Portal-administratorkennwort}
```

Das folgende Beispiel erstellt Endpunktreferenzen auf dem WebSphere Portal-Anwendungsserver für eine Clusterumgebung.

- Beispiel mit Jython:

```
AdminTask.updateEndpointBindingsOnPortal(['-clusterName  
Portal-clustername -endpointBindingDirectoryName  
verzeichnis_mit_endpunktdateien_auf_lokalem_system -host  
IP_oder_hostname_des_Portal-servers -port Portal-SOAP-standardport_8879  
-user Portal-administrator-ID -password Portal-administratorkennwort']])
```

- Beispiel mit Jacl:

```
$AdminTask updateEndpointBindingsOnPortal {-clusterName  
Portal-clustername -endpointBindingDirectoryName  
verzeichnis_mit_endpunktdateien_auf_lokalem_system -host  
IP_oder_hostname_des_Portal-servers -port Portal-SOAP-standardport_8879  
-user Portal-administrator-ID -password Portal-administratorkennwort}
```

### Erforderliche Einträge für die Datei proxy-config.xml zur Konfiguration von Widgets für den kombinierten Einsatz mit WebSphere Portal:

Mit den Beispielen für die erforderlichen Einträge für die Datei proxy-config.xml können Sie den Ajax-Proxy auf dem WebSphere Portal-Server konfigurieren. Um Remote URLs vom WebSphere Portal-Server auf Ihren Produktserver zu ermöglichen, müssen Sie den Ajax-Proxy konfigurieren.

Das folgende XML-Snippet zeigt die Proxy-Richtlinie, die für BPM-Produkte erforderlich ist. Diese muss für alle Remote URLs festgelegt werden, die Sie mit dem WebSphere Portal-Proxy öffnen möchten (z. B. Business Space-Server und BPM-Server). Ersetzen Sie <REMOTE\_BPM\_URL> durch die Remote URL, die mit dem WebSphere Portal-Proxy geöffnet werden soll.

**Tipp:** Der Standardwert für die Socket-Zeitlimitüberschreitung (socket-timeout) liegt bei 10 Sekunden. Business Space verwendet eine Proxy-Serverkomponente, um eine Verbindung zu Ihren REST-Services herzustellen. Wenn die REST-Services nicht antworten, ändern Sie das Socketzeitlimit in einen Wert, der für Ihre Situation

passt, z. B. 30 Sekunden. Vgl. „Einstellung für die Zeitlimitüberschreitung für den Business Space-Ajax-Proxy ändern“ auf Seite 329.

Wenn mehrere ferne Server oder Remote URLs mit dem Proxy für den WebSphere Portal-Server zugelassen werden sollen, passen Sie die Proxy-Konfiguration entsprechend an, indem Sie dynamische Richtlinieneinträge verwenden. Die Proxy-Richtlinie unterscheidet sich von Implementierung zu Implementierung. In der WebSphere Portal-Dokumentation finden Sie verschiedene Verfahren zur Konfiguration des WebSphere Portal-Server-Proxys.

Die Datei proxy-config.xml befindet sich im Verzeichnis *WebSphere\_Portal-installationsstammverzeichnis\base\wp.proxy.config\installableApps\wp.proxy.config.ear\wp.proxy.config.war\WEB-INF*.

**Wichtig:** Die aktualisierte Datei proxy-config.xml muss von Ihren WebSphere Portal-Administratoren geprüft und genehmigt werden, bevor sie in WebSphere Portal eingecheckt wird.

```
<!-- BPM/Business Space-Proxy-Richtlinie -->

<proxy:policy url="<<REMOTE_BPM_URL>" acf="none">
<proxy:actions>
<proxy:method>GET</proxy:method>
<proxy:method>HEAD</proxy:method>
<proxy:method>POST</proxy:method>
<proxy:method>DELETE</proxy:method>
<proxy:method>PUT</proxy:method>

</proxy:actions>
<proxy:cookies>
<proxy:cookie>LtpaToken</proxy:cookie>
<proxy:cookie>LtpaToken2</proxy:cookie>
<proxy:cookie>JSESSIONID</proxy:cookie>
<proxy:cookie>CRN</proxy:cookie>
<proxy:cookie>caf</proxy:cookie>
<proxy:cookie>cam_passport</proxy:cookie>
<proxy:cookie>cc_session</proxy:cookie>
<proxy:cookie>userCapabilities</proxy:cookie>
<proxy:cookie>usersessionid</proxy:cookie>
</proxy:cookies>
<proxy:headers>
<proxy:header>User-Agent</proxy:header>
<proxy:header>Accept*</proxy:header>
<proxy:header>Content*</proxy:header>
<proxy:header>Authorization*</proxy:header>
<proxy:header>X-Method-Override</proxy:header>
<proxy:header>Set-Cookie</proxy:header>
<proxy:header>If-Modified-Since</proxy:header>
<proxy:header>If-None-Match</proxy:header>
<proxy:header>X-Server</proxy:header>
<proxy:header>X-Update-Nonce</proxy:header>
<proxy:header>X-Requested-With</proxy:header>
<proxy:header>com.ibm.lotus.openajax.virtualhost</proxy:header>
<proxy:header>com.ibm.lotus.openajax.virtualport</proxy:header>
<proxy:header>Slug</proxy:header>
<proxy:header>SOAPAction</proxy:header>
</proxy:headers>
</proxy:policy>

<proxy:meta-data>
<proxy:name>forward-http-errors</proxy:name>
<proxy:value>true</proxy:value>
</proxy:meta-data>
```

```
<proxy:meta-data>  
<proxy:name>socket-timeout</proxy:name>  
<proxy:value>30000</proxy:value>  
</proxy:meta-data>
```

## Business Space für den kombinierten Einsatz mit IBM Case Manager konfigurieren

Wenn Ihr Team IBM Case Manager verwendet, können Sie die IBM BPM-Widgets zur Verwaltung von Benutzertasks so konfigurieren, dass sie in einer IBM Case Manager-Umgebung arbeiten. So können die Benutzer ohne Reibungsverluste über ein integriertes Posteingangs-Widget mit IBM BPM-Tasks und IBM Case Manager-Arbeitselementen arbeiten.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

Vor der Konfiguration von Widgets für die Verwaltung von Benutzertasks, die kombiniert mit IBM Case Manager arbeiten sollen, müssen Sie die folgenden Tasks ausführen:

- Installieren und konfigurieren Sie IBM Case Manager V5.1 oder höher zusammen mit Business Space in einer Zelle.
  - Installieren und konfigurieren Sie IBM Business Process Manager Standard oder IBM Business Process Manager Advanced in einer anderen Zelle.
1. Konfigurieren Sie eine zellenübergreifende Sicherheit einschließlich SSO und SSL. Führen Sie „Zellenübergreifende Sicherheit für IBM BPM und IBM Case Manager konfigurieren“ aus.
  2. Registrieren Sie die Widgets in Business Space. Führen Sie abhängig von der Position, an der Business Space konfiguriert ist, eine der folgenden Aktionen aus.
    - Wenn Sie Business Space in IBM Case Manager verwenden, führen Sie die in „IBM BPM-Widgets in IBM Case Manager registrieren“ auf Seite 348 beschriebenen Schritte aus.
    - Wenn Sie Business Space in IBM Business Process Manager Advanced verwenden, führen Sie die in „IBM Case Manager-Widgets in IBM Business Process Manager Advanced registrieren“ auf Seite 351 beschriebenen Schritte aus.
  3. Registrieren Sie die IBM Case Manager REST-Services in IBM BPM. Führen Sie die in „IBM Case Manager REST-Services in IBM BPM registrieren“ auf Seite 352 beschriebenen Schritte aus.
  4. Stellen Sie sicher, dass die erforderliche Föderationsdomäne vorhanden ist. Wenn Sie die Option `-federateSystem true` des Befehls **addICMSystem** im vorhergehenden Schritt nicht zur Erstellung einer Föderationsdomäne namens `BPM_ICM_Federation_Domain` verwendet haben, erstellen Sie jetzt eine solche Domäne, die die Zellen IBM BPM und IBM Case Manager enthält. Dazu dient der Verwaltungsbefehl **createBPMapiFederationDomain**. Sie können einen anderen Domänennamen verwenden.

Nun können Sie ein integriertes Posteingangs-Widget in einem Business Space nutzen.

**Zellenübergreifende Sicherheit für IBM BPM und IBM Case Manager konfigurieren:**

die Produkte werden in zwei verschiedenen Zellen konfiguriert. Beide Zellen müssen auf dieselben Benutzer zugreifen können und benötigen SSO und SSL.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

Bevor Sie eine zellenübergreifende Konfiguration einrichten, müssen Sie die folgenden Tasks ausführen:

- Installieren und konfigurieren Sie IBM Case Manager V5.1 oder höher in einer Zelle.
  - Installieren und konfigurieren Sie IBM Business Process Manager Advanced oder IBM Business Process Manager Standard in einer anderen Zelle.
1. Legen Sie die Konfiguration so an, dass die IBM BPM- und IBM Case Manager-Zellen Zugriff auf dieselben Benutzer haben. Dies kann man auf verschiedenen Wegen erreichen. Die Vorgehensweise ist davon abhängig, welches Repository Sie für Ihr Benutzeraccount gewählt haben. Beispiel: wenn bereits ein LDAP-Server vorhanden ist, können Sie ihn beiden Zellen verfügbar machen.
  2. Ermitteln Sie die erforderlichen Suchfilter, die auf Ihre Benutzerrepositorydefinitionen passen. Beide Zellen erfordern identische Filterzeichenfolgen für die folgenden Suchvorgänge:
    - Benutzer
    - Gruppe
    - Gruppenzugehörigkeit

Sie müssen die Definitionen für Ihr Benutzerrepository überprüfen, damit Sie die korrekten Filterzeichenfolgen festlegen können. Zum Beispiel bei Verwendung eines LDAP-Servers mit den folgenden Definitionen.

- Group: groupOfNames
- OrgContainer: organization;organizationalUnit;domain;container
- PersonAccount: inetOrgPerson

Folgende Suchfilter wären geeignet:

- Benutzersuchfilter: (&(objectClass=inetOrgPerson)(uid={0}))
  - Gruppensuchfilter:  
(&(cn={0})(|(objectClass=groupOfNames)(objectClass=groupOfUniqueNames)))
  - Suchfilter für Gruppenzugehörigkeit: (|( &(objectClass=groupOfNames)(member={0}))( &(objectClass=groupOfUniqueNames)(uniqueMember={0})))
3. Sammeln Sie Informationen über das Benutzerrepository. Stellen Sie in Abhängigkeit des verwendeten Benutzerrepositorytyps geeignete Daten zusammen, z. B. Hostname des Servers, Portnummer, Anmeldeeigenschaft, Zertifikatsabgleich und definierten Namen des LDAP-Basiseintrags.
  4. Fügen Sie auf dem IBM Case Manager-Server das Benutzerverzeichnis zum eingebundenen Realm hinzu.
    - a. Starten Sie Enterprise Manager stellen Sie eine Verbindung zur IBM Case Manager P8-Domäne her.
    - b. Klicken Sie zum Starten des Assistenten für die Erstellung einer Verzeichniskonfiguration, mit der rechten Maustaste auf **Enterprise Manager**, wählen Sie **Eigenschaften** aus, wählen Sie die Registerkarte **Verzeichniskonfiguration** aus und klicken Sie auf **Hinzufügen**. Das Fenster des Assistenten für die Erstellung einer Verzeichniskonfiguration wird geöffnet.

- c. Geben Sie alle Informationen über Ihr Benutzerrepository ein, die der Assistent benötigt.
- d. Fügen Sie einen Basiseintrag für das Benutzerrepository zum eingebundenen Realm hinzu. Klicken Sie in der Administrationskonsole auf **Sicherheit > Globale Sicherheit**, anschließend im Bereich **Benutzeraccountrepository** auf **Konfigurieren > Basiseintrag zum Bereich hinzufügen** und geben Sie anschließend die erforderlichen Informationen zum Benutzerrepository ein. Klicken Sie auf **OK** und anschließend auf **Speichern**.

**Anmerkung:** Vergewissern Sie sich bei Verwendung eines LDAP-Servers, dass Sie EXACT\_DN für den Zertifikatsabgleich angegeben haben.

- e. Starten Sie die IBM Case Manager-Umgebung erneut.
  - f. Prüfen Sie, ob Sie das Benutzerrepository suchen können. Klicken Sie in der Administrationskonsole auf **Benutzer und Gruppen > Benutzer verwalten**. Geben Sie im Bereich **Suche nach Benutzern** eine Zeichenfolge im Feld **Suchen nach** ein, die auf einige der vorhandenen Benutzer im Repository passt, z. B. a\*, klicken Sie auf **Suchen** und prüfen Sie, ob Sie dazu passende Treffer erhalten.
5. Fügen Sie auf dem IBM BPM-Server das Benutzerverzeichnis zum eingebundenen Realm hinzu.
- a. Fügen Sie einen Basiseintrag für das Benutzerrepository zum eingebundenen Realm hinzu. Klicken Sie in der Administrationskonsole auf **Sicherheit > Globale Sicherheit**, anschließend im Bereich **Benutzeraccountrepository** auf **Konfigurieren > Basiseintrag zum Bereich hinzufügen** und geben Sie anschließend die erforderlichen Informationen zum Benutzerrepository ein. Klicken Sie auf **OK** und anschließend auf **Speichern**.

**Anmerkung:** Vergewissern Sie sich bei Verwendung eines LDAP-Servers, dass Sie EXACT\_DN für den Zertifikatsabgleich angegeben haben.

- b. Starten Sie die IBM BPM-Umgebung erneut.
  - c. Prüfen Sie, ob Sie das Benutzerrepository suchen können. Klicken Sie in der Administrationskonsole auf **Benutzer und Gruppen > Benutzer verwalten**. Geben Sie im Bereich **Suche nach Benutzern** eine Zeichenfolge im Feld **Suchen nach** ein, die auf einige der vorhandenen Benutzer im Repository passt, z. B. a\*, klicken Sie auf **Suchen** und prüfen Sie, ob Sie dazu passende Treffer erhalten.
6. Konfigurieren Sie eine zellenübergreifende einmalige Anmeldung (Single Sign-on, SSO).
- a. Vergewissern Sie sich, dass die automatische Schlüsselerstellung abgeschaltet ist. Führen Sie die folgenden Schritte bei allen teilnehmenden Zellen für IBM BPM und IBM Case Manager aus.
    - 1) Klicken Sie in der Administrationskonsole auf **Sicherheit > SSL-Zertifikat und Schlüsselverwaltung > Endpunktsicherheitskonfigurationen verwalten**.
    - 2) Blenden Sie alle Zweige der Baumstruktur entweder bis zum eingehenden oder ausgehenden Gültigkeitsbereich ein, der die Schlüsselsatzgruppe enthält und klicken Sie anschließend auf den Gültigkeitsbereichslink für die Zelle.
    - 3) Klicken Sie im Abschnitt **Verwandte Themen** auf **Schlüsselsatzgruppen**.
    - 4) Klicken Sie auf die Schlüsselsatzgruppe NodeLTPAKeySetGroup.
    - 5) Inaktivieren Sie die Option **Schlüssel automatisch generieren**.

- 6) Klicken Sie auf **OK** und anschließend auf **Speichern**, um die Änderungen in der Masterkonfiguration zu speichern.
  - 7) Starten Sie den Server erneut, damit die Änderungen aktiv werden.
  - 8) Vergessen Sie nicht, die Schritte 6a1 auf Seite 345 bis 6a7 für alle teilnehmenden Zellen beider Produkte auszuführen.
- b. Lassen Sie einen gemeinsamen LTPA-Schlüssel von allen teilnehmenden Zellen gemeinsam nutzen. Als Beispiel dienen die folgenden Schritte zur Darstellung des Exports des LTPA-Schlüssels vom IBM BPM-Server und des Imports in den Schlüsselspeicher einer IBM Case Manager-Zelle.
- 1) Klicken Sie in der Administrationskonsole von IBM BPM auf **Sicherheit > Globale Sicherheit** und anschließend im Abschnitt **Authentifizierung** auf **LTPA**.
  - 2) Geben Sie im Abschnitt **Zellenübergreifende einmalige Anmeldung** ein neues sicheres Kennwort sowie einen Schlüsseldateinamen ein. Die Datei wird im Profilstammverzeichnis des Servers generiert, falls kein vollständig qualifizierter Pfad angegeben wird.
  - 3) Klicken Sie auf **Schlüssel exportieren** und dann auf **OK**.
  - 4) Übertragen Sie die exportierte Schlüsseldatei im Binärmodus auf das Dateisystem der IBM Case Manager-Zelle.
  - 5) Klicken Sie in der Administrationskonsole von IBM Case Manager auf **Sicherheit > Globale Sicherheit** und anschließend im Abschnitt **Authentifizierung** auf **LTPA**.
  - 6) Geben Sie im Abschnitt **Zellenübergreifende einmalige Anmeldung** das Kennwort sowie einen Schlüsseldateinamen ein.
  - 7) Klicken Sie auf **Schlüssel importieren** und dann auf **OK**.
  - 8) Wenn Ihre Konfiguration mehrere Zellen beinhaltet, wiederholen Sie die Schritte 6b4 bis 6b7 für jede weitere Zelle.
- c. Legen Sie den gleichen Domänennamen für SSO fest. Führen Sie die folgenden Schritte bei allen teilnehmenden Zellen von IBM BPM und IBM Case Manager aus.
- 1) Klicken Sie in der Administrationskonsole auf **Sicherheit > Globale Sicherheit**.
  - 2) Erweitern Sie im Abschnitt **Cacheeinstellungen für Authentifizierung** den Bereich **Web- und SIP-Sicherheit**. Klicken Sie anschließend auf **Single sign-on (SSO)**.
  - 3) Geben Sie die folgenden Konfigurationswerte im Abschnitt **Allgemeine Eigenschaften** an:
    - a) Wählen Sie die Option **Aktiviert** aus.
    - b) Geben Sie bei **SSL erforderlich** den Domänennamen an, den Sie aktuell für die Server verwenden, zum Beispiel `beispiel.com`.
    - c) Vergewissern Sie sich dass die Optionen **Interoperabilitätsmodus** und **Web inbound security attribute propagation** (Weitergabe von eingehenden Web-Sicherheitsattributen) beide ausgewählt sind.
    - d) Klicken Sie auf **OK** und speichern Sie Ihre Änderungen in der Masterkonfiguration.
  - 4) Vergessen Sie nicht, die Schritte 6c1 bis 6c3d für alle teilnehmenden Zellen auszuführen.
- d. Vergewissern Sie sich, dass SSO zellenübergreifend arbeitet. Wenn Sie Business Space auf IBM BPM konfiguriert haben, führen Sie die folgenden Aktionen aus:



- 1) Öffnen Sie mit einem Web-Browser den IBM BPM Business Space-Client, indem Sie eine ähnlich lautende URL eingeben wie im folgenden Beispiel: `http://bpmserver.example.com:9080/BusinessSpace`.
  - 2) Melden Sie mit einem Benutzernamen und einem Kennwort an, das auf dem gemeinsam genutzten LDAP-Server gespeichert ist.
  - 3) Drücken Sie - ohne die Registerkarte IBM BPM Business Space zu schließen, **STRG-T**, um eine neue Registerkarte im Browser zu öffnen.
  - 4) Öffnen Sie in der neuen Registerkarte des Browsers den IBM Case Manager-Case-Client, indem Sie eine ähnlich lautende URL eingeben wie im folgenden Beispiel: `http://icmserver.example.com:9080/CaseClient`.
  - 5) Wenn Sie automatisch als derselbe Benutzer angemeldet sind ohne im Case-Client eine Benutzer-ID und Kennwort einzugeben, dann funktioniert SSO.
7. SSL durch den Austausch der serverbasierter SSL-Zertifikate konfigurieren
- a. Extrahieren Sie das Stamm-SSL-Zertifikat vom IBM BPM-Server. Führen Sie über die Administrationskonsole auf dem IBM BPM-Server folgende Aktionen aus.
    - 1) Klicken Sie auf **Sicherheit > SSL-Zertifikat und Schlüsselverwaltung > Schlüsselspeicher und Zertifikate > DefaultTrustStore > Unterzeichnerzertifikate**.
    - 2) Wählen Sie das Stammzertifikat aus und klicken Sie anschließend auf **Extrahieren**.
    - 3) Geben Sie einen Dateinamen für das exportierte Zertifikat ein, z. B. `c:\bpmserverCert.pem`, und klicken Sie auf **OK**.

**Anmerkung:** Wenn Sie eine Rechnerverbindung über Fernzugriff nutzen, wird das exportierte Zertifikat auf der Maschine gespeichert, von der aus Sie die Administrationskonsole gestartet haben.
  - b. Übertragen Sie die exportierte Zertifikatsdatei im Binärmodus auf das Dateisystem von IBM Case Manager.
  - c. Fügen Sie das IBM BPM-Serverzertifikat zum IBM Case Manager-Server hinzu. Führen Sie über die Administrationskonsole auf dem IBM Case Manager-Server folgende Aktionen aus.
    - 1) Klicken Sie auf **Sicherheit > SSL-Zertifikat und Schlüsselverwaltung > Schlüsselspeicher und Zertifikate > DefaultTrustStore > Unterzeichnerzertifikate**.
    - 2) Klicken Sie auf **Hinzufügen**.
    - 3) Geben Sie einen Aliasnamen ein, beispielsweise `bpmserver`.
    - 4) Geben Sie einen Dateinamen für das IBM BPM-Serverzertifikat ein, z. B. `c:\bpmserverCert.pem`, und klicken Sie auf **OK**.
    - 5) Speichern Sie die Änderungen.
  - d. Extrahieren Sie das Stamm-SSL-Zertifikat vom IBM Case Manager-Server. Führen Sie über die Administrationskonsole auf dem IBM Case Manager-Server folgende Aktionen aus.
    - 1) Klicken Sie auf **Sicherheit > SSL-Zertifikat und Schlüsselverwaltung > Schlüsselspeicher und Zertifikate > DefaultTrustStore > Unterzeichnerzertifikate**.
    - 2) Wählen Sie das Stammzertifikat aus und klicken Sie anschließend auf **Extrahieren**.
    - 3) Geben Sie einen Dateinamen für das exportierte Zertifikat ein, z. B. `c:\icmserverCert.pem`, und klicken Sie auf **OK**.

**Hinweis:** Wenn Sie eine Rechnerverbindung über Fernzugriff nutzen, wird das exportierte Zertifikat auf der Maschine gespeichert, von der aus Sie die Administrationskonsole gestartet haben.

- e. Übertragen Sie die exportierte Zertifikatsdatei im Binärmodus auf das Dateisystem von IBM BPM.
- f. Fügen Sie das IBM Case Manager-Serverzertifikat zum IBM BPM-Server hinzu. Führen Sie über die Administrationskonsole auf dem IBM BPM-Server folgende Aktionen aus.
  - 1) Klicken Sie auf **Sicherheit > SSL-Zertifikat und Schlüsselverwaltung > Schlüsselspeicher und Zertifikate > DefaultTrustStore > Unterzeichnerzertifikate**.
  - 2) Klicken Sie auf **Hinzufügen**.
  - 3) Geben Sie einen Aliasnamen ein, beispielsweise `icmsserver`.
  - 4) Geben Sie einen Dateinamen für das IBM BPM-Serverzertifikat ein, z. B. `c:\icmsserverCert.pem`, und klicken Sie auf **OK**.
  - 5) Speichern Sie die Änderungen.

Die zellenübergreifende Sicherheit wurde nun eingerichtet, einschließlich SSO und SSL.

Registrieren Sie die IBM BPM-Widgets in IBM Case Manager.

#### **IBM BPM-Widgets in IBM Case Manager registrieren:**

Registrieren Sie den Widgetkatalog und die Endpunkte.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

Sie haben IBM Business Process Manager Advanced und IBM Case Manager in in einer zellenübergreifenden Konfiguration eingerichtet; dazu gehört ein eingebundener Realm, Single-Sign-on und Secure Socket Layer.

1. Wenn Sie IBM BPM Standard oder ein IBM BPM Advanced-Profil ohne Business Space verwenden, müssen Sie die Widgetanwendung zur Benutzertaskverwaltung auf dem IBM BPM-Server oder Cluster installieren.
  - a. Verwenden Sie den Befehl **installHumanTaskManagementWidgets** zur Installation der Widgetanwendung zur Benutzertaskverwaltung auf dem IBM BPM-Server oder Cluster. Zur Installation der Widgetanwendung zur Benutzertaskverwaltung auf dem Cluster Support können Sie die folgenden Jython-Befehle absetzen:

```
AdminTask.installHumanTaskManagementWidgets('-clusterName Support')
AdminConfig.save()
```
  - b. Suchen Sie über die Administrationskonsole die Widgetanwendung zur Benutzertaskverwaltung namens `HumanTaskManagementWidgets_geltungsbereich` und starten Sie sie.
2. Wenn Sie BPEL-Tasks in IBM BPM Advanced verwenden, müssen Sie dort, wo die Widgetanwendung zur Benutzertaskverwaltung installiert ist, auch Dojo-Formulare einsetzen.
3. geben Sie auf dem IBM BPM-Server den Hostnamen und die Ports für die eingebundene REST API von IBM BPM an. Da die Widgets sowohl HTTP als auch HTTPS-Protokolle verwenden, beachten Sie die Portnummern für beide Protokolle.

- Wenn Sie auf Ihre Webmodule aus Gründen des Lastausgleichs oder zur höheren Verfügbarkeit über einen HTTP-Server zugreifen, verwenden Sie den Hostnamen und die Porteinstellungen des HTTP-Servers.
  - Bei einem eigenständigen IBM BPM-Server müssen Sie dessen Hostnamen verwenden. Zur Angabe der Portnummern klicken Sie in der Administrationskonsole auf **Server > Servertypen > WebSphere-Anwendungsserver > servername** und blenden Sie dann den Abschnitt **Ports** ein. Der Standardport **wc\_defaulthost** wird für HTTP-Verbindungen und der (sichere) Port **wc\_defaulthost\_secure** für HTTPS-Verbindungen verwendet.
4. Kopieren Sie die folgenden Dateien vom IBM BPM-Server auf den IBM Case Manager-Server.
    - `installationsstammverzeichnis\BusinessSpace\registryData\BPM\BPM_HumanTaskManagement_crosscell.zip`
    - Wenn Sie auch IBM BPM Advanced einsetzen, kopieren Sie auch die ZIP-Datei `installationsstammverzeichnis\BusinessSpace\registryData\BPM\BPM_HumanTaskManagement_Advanced_crosscell.zip`
  5. Erstellen Sie ein neues Verzeichnis.
  6. Entpacken Sie alle ZIP-Dateien in das neue Verzeichnis. Vergewissern Sie sich, dass folgende Verzeichnisse vorhanden sind:
    - catalog
    - endpoints
    - templates
  7. Definieren Sie die Endpunkte für die REST-Services. Führen Sie die folgenden Schritte aus.
    - a. Wechseln Sie in das Verzeichnis endpoints. Es sollte folgende Dateien enthalten.
      - `HumanTaskManagementEndpoints.xml` mit den Endpunkten für Prozess- und Task-Services.
      - `HumanTaskManagementWidgetsEndpoint.xml` mit den Endpunkten für die Widgets für die Benutzertaskverwaltung und die vordefinierten Task-Formulare. Diese müssen beide auf den Hostnamen und die Portnummer für das IBM BPM-Implementierungsziel konfiguriert sein, in dem Business Space implementiert ist oder für das der Befehl **installHumanTaskManagementWidgets** ausgeführt wurde.
      - `wsumEndpoint.xml` mit dem Endpunkt für die Benutzerzugehörigkeitsservices.
    - b. Bearbeiten Sie alle Endpunkt-XML-Dateien im Verzeichnis endpoints. Suchen Sie in jeder Datei nach den `<tns:Endpoint>`-Tags, und ändern Sie den Wert für `<tns:url>` in den vollständig qualifizierten Hostnamen und die entsprechende Portnummer für die IBM BPM-REST API.  
 Beispiel: Wenn der Hostname Ihres Servers auf `bpmserver.example.com` lautet und er Port 9080 verwendet, müssen Sie die Endpunkt-URLs für Business Flow Manager (BFM) und Human Task Manager (HTM) in die eingebundenen Versionen dieser URLs ändern.
      - Für BFM: `http://bpmserver.example.com:9080/rest/bpm/federated/bfm`
      - Für HTM: `http://bpmserver.example.com:9080/rest/bpm/federated/htm`

**Tipp:** Sie können die URLs für die REST-Services über die Administrationskonsole nachsehen, indem Sie auf **Services > REST-Services > REST-Services** klicken.

8. Wenn Sie IBM Business Process Manager Advanced einsetzen und Ihre eigenen BPEL-Prozessanwendungen Dojo-Formulare verwenden, müssen Sie für jedes Webmodul, das diese Dojo-Formulare enthält, einen Endpunkt registrieren. Führen Sie für jedes Webmodul folgende Schritte aus.
  - a. Erstellen Sie eine eindeutig benannte Kopie von `installationsstammverzeichnis\BusinessSpace\registryData\BPM\endpoints\CustomFormsEndpoint.xml` im Verzeichnis `endpoints`, das im Schritt 6 auf Seite 349 angelegt wurde.
  - b. Bearbeiten Sie die Endpunktdatei, die Sie gerade kopiert haben.
    - 1) Aktualisieren Sie die Werte `tns:id` und `tns:type` mit einen eindeutigen Namen für Ihr Webmodul. Beispiel: `{com.example}myForms`.
    - 2) Aktualisieren Sie den Wert `tns:url` mit genau den gleichen Angaben für Protokoll, Hostnamen und Portnummer, die Sie im Schritt 7 auf Seite 349 für den Endpunkt der Widgets zur Benutzertaskverwaltung festgelegt haben. Verwenden Sie das Kontextstammverzeichnis des Webmoduls, das Ihre Dojo-Formulare enthält.
9. Importieren Sie auf dem IBM Case Manager-Server in einer `wsadmin`-Sitzung den Widgetkatalog und die Endpunktdefinitionen, indem Sie folgende Jython-Befehle ausführen:
 

```
AdminTask.updateBusinessSpaceWidgets('[-nodeName knotenname -serverName servername
  -catalogs verzeichnis_mit_der_katalogdatei
  -endpoints verzeichnis_mit_den_endpunktdateien
  -templates verzeichnis_mit_den_vorlagendateien]')
```

```
AdminConfig.save()
```

Dabei sind `knotenname` und `servername` die Bezeichnungen des Knotens und Servers für den IBM Case Manager-Server. Verwenden Sie bei einem Cluster den Parameter `-clusterName` anstelle von `-nodeName` und `-serverName`. Weitere Informationen zum Befehl `updateBusinessSpaceWidgets` finden Sie, wenn Sie dem Link zu den Referenzinformationen folgen.
10. Starten Sie den IBM Case Manager Server erneut.

Die Business Space-Widgets sind in IBM Case Manager registriert.

Konfigurieren Sie die IBM Case Manager-Services in IBM BPM.

*Befehl `installHumanTaskManagementWidgets`:*

Verwenden Sie den Befehl `installHumanTaskManagementWidgets`, um die Widgetanwendung zur Benutzertaskverwaltung auf einem IBM BPM Standard- oder IBM BPM Advanced-Server bzw. -Cluster zu installieren.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced ohne konfigurierten Business Space

Wenn Sie Widgets zur Benutzertaskverwaltung in einer zellenübergreifenden Konfiguration mit IBM Case Manager verwenden möchten, nehmen Sie den Befehl `installHumanTaskManagementWidgets`, um nur die erforderliche Widgetanwendung zu installieren.

#### Erforderliche Parameter

`-clusterName` *clustername*

Dieser Parameter gibt den Namen des IBM BPM-Clusters an, in dem die Wid-

getanwendung zur Benutzertaskverwaltung installiert wird. Normalerweise sollte es sich dabei um den Cluster handeln, in dem Business Space installiert wäre. Beispiel: den Anwendungscluster in einer Topologie mit einem oder zwei Clustern, den Unterstützungscluster in einer Topologie mit drei Clustern und den Webanwendungscluster in einer Topologie mit vier Clustern.

Wenn Sie den Parameter **clusterName** angeben, dann geben nicht zugleich die beiden Parameter **serverName** und **nodeName** an.

**-nodeName** *knotenname*

Dieser Parameter gibt den Namen des IBM BPM-Knotens an, in dem die Wid-  
getanwendung zur Benutzertaskverwaltung installiert ist. Wenn Sie den Para-  
meter **clusterName** nicht angeben, müssen Sie die beiden Parameter **serverName**  
und **nodeName** setzen.

**-serverName** *servername*

Dieser Parameter gibt den Namen des IBM BPM-Servers an, in dem die Wid-  
getanwendung zur Benutzertaskverwaltung installiert wird. Wenn Sie Business  
Space später auf dem selben Server konfigurieren, auf dem die Widgetanwen-  
dung zur Benutzertaskverwaltung installiert ist, wird die vorhandene Anwen-  
dung dann von Business Space verwendet. Wenn Sie den Parameter  
**clusterName** nicht angeben, müssen Sie die beiden Parameter **serverName** und  
**nodeName** setzen.

## Beispiel

Im folgenden Beispiel wird der Befehl **installHumanTaskManagementWidgets** ver-  
wendet, um die Widgetanwendung zur Benutzertaskverwaltung auf demSupport-  
Cluster zu installieren.

Beispiel mit Jython:

```
AdminTask.installHumanTaskManagementWidgets('-clusterClusterName Support')  
AdminConfig.save()
```

Beispiel mit Jacl:

```
$AdminTask installHumanTaskManagementWidgets {-clusterClusterName Support}  
$AdminConfig save
```

## IBM Case Manager-Widgets in IBM Business Process Manager Advanced registrieren:

Zur Verwendung eines integrierten Posteingangs-Widgets in der Business Space-  
Konfiguration in IBM Business Process Manager Advanced müssen Sie die IBM  
Case Manager-Widgets in IBM Business Process Manager Advanced registrieren.

**Geltungsbereich des Themas:** Dieser Abschnitt gilt für IBM Business Process Ma-  
nager Advanced.

Sie haben IBM Business Process Manager Advanced und IBM Case Manager in in  
einer zellenübergreifenden Konfiguration eingerichtet; dazu gehört ein eingebunde-  
ner Realm, Single-Sign-on und Secure Socket Layer. Business Space ist in IBM Busi-  
ness Process Manager Advanced konfiguriert.

1. Kopieren Sie den Inhalt des Verzeichnisses

```
CASE_MANAGEMENT_INSTALLATION_PATH/CaseWidgets/BusinessSpace/  
ConnectorForIBM_BPM_WidgetRegistration/ vom IBM Case Manager-Server auf  
den IBM BPM-Server. Dieses Verzeichnis enthält die Unterverzeichnisse catalog  
und endpoints.
```

2. Definieren Sie die Endpunkte für die REST-Services. Führen Sie die folgenden Schritte aus.
  - a. Wechseln Sie in das Verzeichnis endpoints.
  - b. Bearbeiten Sie die Datei `acmwidgetsEndPoints.xml` und aktualisieren Sie die URL so, dass sie auf die IBM Case Manager-Widgets verweist.
3. Importieren Sie auf dem IBM BPM-Server in einer wsadmin-Sitzung den Widgetkatalog und die Endpunktdefinitionen, indem Sie folgende Jython-Befehle ausführen:

```
AdminTask.updateBusinessSpaceWidgets('[-nodeName knotenname -serverName servername
  -catalogs verzeichnis_mit_der_katalogdatei
  -endpoints verzeichnis_mit_endpunktdateien]')
AdminConfig.save()
```

Dabei sind *knotenname* und *servername* die Bezeichnungen des Knotens und Servers für den IBM Business Process Manager Advanced-Server. Verwenden Sie bei einem Cluster den Parameter **-clusterName** anstelle von **-nodeName** und **-serverName**.

4. Starten Sie den IBM Business Process Manager Advanced Server erneut.

Der Connector für das IBM BPM-Widget wird in IBM Business Process Manager Advanced registriert. Wenn Sie sich bei Business Space anmelden, ist der Connector für das IBM BPM-Widget verfügbar.

Konfigurieren Sie die IBM Case Manager-Services in IBM BPM.

#### IBM Case Manager REST-Services in IBM BPM registrieren:

Führen Sie den Befehl **addICMSystem**dort aus, wo die IBM BPM eingebundene REST API implementiert ist.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

1. Bestimmen Sie die die folgenden Werte für Ihr IBM Case Manager-System.
  - Zellenname
  - Knoten- und Servernamen oder Clustername
  - Verbindungsname der Prozessengine
  - Hostname
  - Portnummer
  - das verwendete Übertragungsprotokoll (HTTP oder HTTPS)
2. Entscheiden Sie, ob Ihr IBM Case Manager-System zur Föderationsdomäne für IBM BPM und IBM Case Manager hinzugefügt werden soll. Verwenden Sie dazu die Option `-federateSystem true` für den Befehl **addICMSystem**. Alternativ können Sie erst später eine geeignete Föderationsdomäne erstellen.
3. Führen Sie den Befehl **addICMSystem**dort aus, wo die IBM BPM eingebundene REST API implementiert ist. Folgende Beispiele fügen HTTPS-Endpunkte für IBM Case Manager-Services zu einem IBM Business Process Manager Advanced-Cluster hinzu und erstellen die Föderationsdomäne `BPM_ICM_Federation_Domain` mit zwei Systemen, ICM und BPM.

Beispiel mit Jython:

```
AdminTask.addICMSystem('[-icmCellName zellenname
  -icmClusterName clustername
  -PEConnectionName verbindungsname
```



```
-icmHostName hostname  
-icmPort port  
-icmTransportType https  
-federateSystem true]')
```

Beispiel mit Jacl:

```
$AdminTask addICMSystem {-icmCellName zellename  
-icmClusterName clustername  
-PEConnectionName verbindungsname  
-icmHostName hostname  
-icmPort port  
-icmTransportType https  
-federateSystem true}
```

Die IBM Case Manager REST-Services werden in IBM BPM registriert.

*Befehl addICMSystem:*

Verwenden Sie den Befehl **addICMSystem** um Endpunkte für IBM Case Manager-Services zur Endpunktregistrierungsdatei für IBM BPM hinzuzufügen. Damit kann die eingebundene REST API auf dem IBM BPM Advanced-Server mit dem IBM Case Manager -Server eine Verbindung aufbauen.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

Dieser Befehl muss dort ausgeführt werden, wo die IBM BPM eingebundene REST API implementiert ist. Geben Sie bei der Ausführung dieses Befehls auch die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

#### **Erforderliche Parameter**

**-icmCellName** *zellename*

Ein Parameter, der den Namen der IBM Case Manager-Zelle angibt.

**-icmNodeName** *knotenname*

Ein Parameter, der den Namen des IBM Case Manager-Knoten für die Konfiguration angibt. Wenn Sie den Parameter **icmClusterName** nicht angeben, müssen Sie die beiden Parameter **icmServerName** und **icmNodeName** setzen.

**-icmServerName** *servername*

Ein Parameter, der den Namen des IBM Case Manager-Servers für die Konfiguration angibt. Wenn Sie den Parameter **icmClusterName** nicht angeben, müssen Sie die beiden Parameter **icmServerName** und **icmNodeName** setzen.

**-icmClusterName** *clustername*

Ein Parameter, der den Namen des IBM Case Manager-Clusters für die Konfiguration angibt. Zur Konfiguration von Business Space auf einem Cluster müssen Sie den Parameter **icmClusterName** ohne die Parameter **icmServerName** und **icmNodeName** angeben.

**-PEConnectionName** *verbindungsname*

Ein Parameter, der den Verbindungsnamen für die Prozessengine von IBM Case Manager angibt.

**-icmHostName** *hostname*

Ein Parameter, der den Namen des IBM Case Manager-Hosts angibt.

**-icmPort** *port*

Ein Parameter, der die Portnummer des IBM Case Manager-Hosts angibt.

### **-icmTransportType http | https**

Ein Parameter, der angibt, ob die eingebundene REST API das HTTP- oder das HTTPS-Protokoll verwendet.

### **Optionale Parameter**

#### **-federateSystem true | false**

Wenn dieser Parameter auf true (wahr) gesetzt wird, wenn die Einbindungsdomäne namens `BPM_ICM_Federation_Domain` nicht existiert, wird er mit zwei Systemen - ICM und BPM - erstellt. Standardmäßig ist false (falsch) gesetzt; dies bedeutet, es wird keine Domäne erstellt oder verändert. Sie können die Domäne auch mithilfe der vorhandenen Befehle zur Einbindung von Domänen, beispielsweise `modifyBPMApiFederationDomain` verwenden.

### **Beispiel**

Die folgenden Beispiele verwenden den Befehl **addICMSystem**, um HTTPS-Endpunkte für IBM Case Manager-Services in IBM BPM hinzuzufügen, ohne IBM Case Manager zu einer eingebundenen Domäne hinzuzufügen.

Beispiel mit Jython:

```
AdminTask.addICMSystem(['-icmCellName zellename  
-icmClusterName clustername  
-PEConnectionName verbindungsname  
-icmHostName hostname  
-icmPort port  
-icmTransportType https  
-federateSystem false']])
```

Beispiel mit Jacl:

```
$AdminTask addICMSystem {-icmCellName zellename  
-icmClusterName clustername  
-PEConnectionName verbindungsname  
-icmHostName hostname  
-icmPort port  
-icmTransportType https  
-federateSystem false}
```

*Befehl removeICMSystem:*

Verwenden Sie den Befehl **removeICMSystem** zur Entfernung von Endpunkten für IBM Case Manager-Services aus der Endpunktregistrierungsdatei für IBM BPM.

**Geltungsbereich des Themas:** Dieses Thema gilt für die folgenden Produkte:

- IBM Business Process Manager Standard
- IBM Business Process Manager Advanced

Dieser Befehl muss dort ausgeführt werden, wo die IBM BPM eingebundene REST API implementiert ist. Geben Sie die Option `-conntype NONE` an, wenn der Anwendungsserver nicht aktiv ist.

Obwohl der Befehl **addICMSystem** zum Hinzufügen eines IBM Case Manager-Systems zu einer Föderationsdomäne verwendet werden kann, ist es nicht umgekehrt möglich, den Befehl **removeICMSystem** zum Entfernen eines Implementierungsziels aus einer Föderationsdomäne zu verwenden. Für diese Task dienen die Verwaltungsbefehle für Föderationsdomänen.

### Erforderliche Parameter

**-icmCellName** *zellename*

Ein Parameter, der den Namen der IBM Case Manager-Zelle angibt.

**-icmNodeName** *knotenname*

Ein Parameter, der den Namen des IBM Case Manager-Knotens angibt. Geben Sie entweder die beiden Parameter **icmServerName** und **icmNodeName** an oder nur den Parameter **icmClusterName**.

**-icmServerName** *servername*

Ein Parameter, der den Namen des IBM Case Manager-Servers angibt. Geben Sie entweder die beiden Parameter **icmServerName** und **icmNodeName** an oder nur den Parameter **icmClusterName**.

**-icmClusterName** *clustername*

Ein Parameter, der den Namen des IBM Case Manager-Clusters angibt. Geben Sie entweder die beiden Parameter **icmServerName** und **icmNodeName** an oder nur den Parameter **icmClusterName**.

**-PEConnectionName** *verbindungsname*

Ein Parameter, der den Verbindungsnamen für die Prozessengine von IBM Case Manager angibt.

### Beispiel

Das folgende Beispiel verwendet den Befehl **removeICMSystem** zum Entfernen der IBM Case Manager-Endpunkte für IBM Case Manager-Services in einem Cluster.

Beispiel mit Jython:

```
AdminTask.removeICMSystem(['-icmCellName zellename  
-icmClusterName clustername  
-PEConnectionName verbindungsname'])
```

Beispiel mit Jacl:

```
$AdminTask removeICMSystem {-icmCellName zellename  
-icmClusterName clustername  
-PEConnectionName verbindungsname}
```

---

## Globales Prozess-Monitormodell konfigurieren

Das globale Prozess-Monitormodell bietet die Möglichkeit, einen beliebigen BPEL-Prozess und Benutzertasks zu überwachen, ohne Schritte zur Generierung von Monitormodellen oder zur Implementierung auszuführen. Prozesse werden dynamisch erkannt und auf der Basis der von ihnen ausgegebenen Ereignisse verfolgt. Die erfassten Daten können in Business Space mithilfe der Instanzen, KPIs und der Widgets für die Berichterstellung angezeigt werden.

Informationen zur Verwendung des globalen Prozess-Monitormodells finden Sie unter Globaler Prozess-Monitor auf der Website mit Beispielen und Lernprogrammen zum Geschäftsprozessmanagement (Business Process Management Samples and Tutorials) oder im developerWorks-Artikel, der über den zugehörigen Informationslink zur Verfügung steht.

## Globales Prozess-Monitormodell manuell installieren

Wenn Sie das globale Prozess-Monitormodell bei der Erstellung des IBM Business Monitor-Profiles nicht installiert haben, können Sie diese Komponente zu einem späteren Zeitpunkt anhand der folgenden Schritte installieren. Die Datei

GlobalProcessMonitorV75.ear ist bereits auf Ihrer Festplatte gespeichert, auch wenn Sie das globale Prozess-Monitormodell während der Profilerstellung nicht installiert haben. Verwenden Sie die Administrationskonsole, um diese Datei zu installieren.

Führen Sie die folgenden Schritte aus, um die Datei GlobalProcessMonitorV75.ear zu installieren:

1. Klicken Sie in der Administrationskonsole auf **Anwendungen > Monitormodelle**. In dieser Tabelle werden alle derzeit installierten Monitormodelle aufgelistet.
2. Klicken Sie auf **Installieren**.
3. Wählen Sie **Lokales Dateisystem** aus und klicken Sie auf **Durchsuchen**.
4. Navigieren Sie zu dem Ordner, der die EAR-Datei enthält: application\_server-stammverzeichnis/installableApps.wbm/monitorModels. Wählen Sie dort GlobalProcessMonitorV75.ear aus und klicken Sie auf **Öffnen**.
5. Vergewissern Sie sich, dass die Option 'Nur anfragen, wenn zusätzliche Informationen erforderlich sind' ausgewählt wurde.
6. Klicken Sie auf **Weiter** und akzeptieren Sie alle Standardwerte, bis Sie die Übersichtsseite erreichen.
7. Überprüfen Sie auf der Seite 'Zusammenfassung', ob alle Informationen korrekt sind, und klicken Sie dann auf **Fertig stellen**.
8. Optional: Klicken Sie auf die Option zum **Überprüfen der Änderungen**, um die Daten zu überprüfen, bevor Sie diese speichern oder verwerfen.
9. Klicken Sie auf **Speichern**, um die Änderungen in der Masterkonfiguration und das Modell zu speichern.

Wenn die Prozesse, die Sie überwachen möchten, auf demselben Server ausgeführt werden, ist keine weitere Konfiguration erforderlich. Andernfalls muss das Monitormodell wie im Abschnitt 'Empfang von Ereignissen konfigurieren' beschrieben für den Empfang von Ereignissen vom fernen CEI (IBM Business Process Manager) sowie vom lokalen CEI (IBM Business Monitor-Server) konfiguriert werden, da das globale Prozess-Monitormodell Ereignisse an sich selbst sendet.

## Ereignisse für das globale Prozess-Monitormodell aktivieren

Um den globalen Prozess-Monitor für die Überwachung von Prozessen und Benutzertasks zu aktivieren, ist die Aktivierung der Generierung von BPEL-Ereignissen mithilfe von Integration Designer erforderlich. Durch die von Ihnen aktivierten Ereignisse wird festgelegt, wie viele Informationen IBM Business Monitor über die aktiven Prozesse und Benutzertasks erhält. Die Ereignisgenerierung für IBM Business Process Manager ist standardmäßig ausgewählt.

Die folgenden Vorschläge stellen allgemeine Empfehlungen dar, welche BPEL-Ereignisse aktiviert werden sollten:

- Aktivieren Sie für jeden Prozess, der überwacht werden soll, alle Ereignisse auf der Verarbeitungsebene. In der Regel gibt ein Prozess während der Ausführung nur wenige Ereignisse aus (Start, Ende, Fehler, Löschen).
- Aktivieren Sie für jede Aktivität, die für Sie von Interesse ist (in der Regel Mitarbeiteraktivitäten und Aufrufe), ebenfalls alle Ereignisse.
- Für jede Mitarbeiteraktivität, die überwacht werden soll, wechseln Sie zur Registerkarte 'Details' der Sicht 'Eigenschaften' und suchen den Link zur entsprechenden Benutzertask (falls kein entsprechender Link vorhanden ist, klicken Sie auf die Schaltfläche 'Öffnen', um einen Link zu erstellen). Folgen Sie dem Link zur

Benutzertask, wechseln Sie zur Registerkarte 'Ereignisüberwachung' der Sicht 'Eigenschaften' und aktivieren Sie dann die erforderlichen Prüfereignisse.

- Wenn Sie sowohl einen Prozess als auch einen durch diesen Prozess aufgerufenen Unterprozess überwachen, aktivieren Sie alle Ereignisse für die Aufrufaktivität, die beide Prozesse verknüpft.
- Inaktivieren Sie Ereignisse für automatisierte Schritte mit kurzer Laufzeit.
- Aktivieren Sie alle Ereignisse für die eigenständigen Benutzertasks, die Sie überwachen möchten.
- Ziehen Sie die Aktivierung aller Ereignisse für Schleifen in Betracht. Sie erhalten dadurch ein Protokoll von Iterationsschleifen mit Zeitmarke.
- Aktivieren Sie variable Änderungsereignisse für die Prozessvariablen, die Sie überwachen möchten, nicht jedoch für andere Prozessvariablen.

Weitere Informationen zum Aktivieren der Ereignisgenerierung finden Sie in der Dokumentation zu Integration Designer 8.0. Ein entsprechender Link ist unten angeführt.

## Dashboards für das globale Prozess-Monitormodell konfigurieren

Der globale Prozess-Monitor empfängt Ereignisse zu Prozessen und Benutzertasks, die in IBM Business Process Manager ausgeführt werden. Er erkennt implementierte Prozess- und Taskdefinitionen aufgrund der Ereignisse, die diese während der Ausführung ausgeben und überwacht die aktiven Prozesse und Tasks. Sie können mithilfe der Instanzen, KPIs und der Widgets für die Berichterstellung Ihr eigenes Dashboard für dieses Monitormodell einrichten oder einen der bereitgestellten Business Spaces als Ausgangspunkt verwenden.

In den folgenden Verzeichnissen sind zwei Business Space-Konfigurationen zu finden:

- `application_server-stammverzeichnis/installableApps.wbm/monitorModels/BusinessSpace/GlobalProcessMonitor_BusinessSpace.zip`
- `application_server-stammverzeichnis/installableApps.wbm/monitorModels/BusinessSpace/GlobalProcessMonitor_BusinessSpace_Advanced.zip`

Beide Konfigurationen besitzen dieselbe Gesamtstruktur, die erweiterte Version verfügt jedoch über zusätzliche technische Details wie Millisekundengenauigkeit und Zeitoneninformationen für Zeitmarken, Prozess- und Taskinstanzkennungen, Prozessinstanz-Migrationsprotokolle und Prüfereigniszähler. Laden Sie die gewünschte Konfiguration über die Importfunktion in Business Space hoch. Sie können sie ohne Wartung (auf „as-is“-Basis) verwenden oder als Ausgangspunkt nutzen, um Ihre personalisierten Dashboardsichten zu konfigurieren.

Zur ersten Orientierung kann es hilfreich sein, die Monitoring-Kontext-Struktur dieses Modells zu verstehen:

```
Process Definition
  Process Execution
    Process Execution Step
      Related Task Execution
    Process Execution Variable
  Step Definition
    Step Execution
      Related Task Execution

Task Definition
  Task Execution
```

Es sind zusätzliche Monitoring-Kontextdefinitionen für Daten vorhanden, die nicht in einen Messwert aufgenommen werden konnten und deshalb untergeordnete Monitoring-Kontexte benötigen. Diese können als Datencontainer betrachtet werden, die Teil des entsprechenden übergeordneten Monitoring-Kontexts sind. Sie werden in der obigen Struktur nicht angezeigt, die nur die übergeordnete Monitoring-Kontextstruktur dieses Monitormodells hervorhebt.

Ein 'Process Definition'-Monitoring-Kontext entspricht einer implementierten Prozessvorlage in IBM Business Process Manager. Er überwacht diese Vorlage und stellt Übersichtsdaten zur Anzahl der gestarteten, aktiven und abgeschlossenen Prozesse sowie der minimalen, maximalen und durchschnittlichen Laufzeit etc. bereit. Wenn Sie nach unten zu einem 'Process Execution'-Monitoring-Kontext navigieren, finden Sie Informationen zu einer bestimmten Prozessausführung (Startzeit, aktueller Status, Fertigstellungszeit etc.) Die untergeordneten Elemente eines 'Process Execution'-Kontexts sind die Monitoring-Kontexte der einzelnen Kontextschritte (Aktivitäten, Benutzertasks etc.) sowie die Prozessvariablen.

Alternativ können Sie auch von einem 'Process Definition'-Monitoring-Kontext zu seinen untergeordneten 'Step Definition'-Monitoring-Kontexten navigieren, um alle bekannten Schritte dieses Prozesses anzuzeigen. (Ausschließlich Schritte, die mindestens einmal ausgeführt wurden und Ereignisse an IBM Business Monitor gesandt haben, können erkannt werden.) Wenn Sie noch weiter nach unten navigieren, erreichen Sie die 'Step Execution'-Ebene, auf der dieselben Informationen wie auf der 'Process Execution Step'-Ebene zu finden sind, allerdings in anderer Gruppierung. Hier finden Sie alle Ausführungen einer bestimmten Schrittdefinition und nicht alle Schritte, die zu einer Prozessausführung gehören.

Bei der Konfiguration von Dashboards (entweder Ihre eigenen angepassten Dashboards oder die bereitgestellten Dashboards) können Sie auswählen, welche Messwerte in den Widgets angezeigt werden sollen. Messwerte mit dem Präfix Aux im Messwertnamen werden nur zur internen Verarbeitung verwendet und sollten nicht in das Dashboard eingefügt werden.



---

## Kapitel 11. Präsentationsmodell installieren

Die Einzelserverversion von IBM Business Monitor enthält ein Mustermodell für die Bearbeitung von Hypothekendarlehen ('Better Lender'), das einen Teil der Funktionalität von IBM Business Monitor veranschaulicht. Wenn Sie ein eigenständiges Profil erstellt haben, können Sie das Präsentationsmodell 'Better Lender' über die Konsole 'Erste Schritte' installieren.

Zur Installation des Präsentationsmodells 'Better Lender' aus der Einstiegskonsole müssen Sie sicherstellen, dass IBM Cognos Business Intelligence installiert und gestartet ist.

Das Präsentationsmodell 'Better Lender' befindet sich im folgenden Verzeichnis:

```
application_server-stammverzeichnis/installableApps.wbm/samples/  
mortgageLending/  
application_server-stammverzeichnis\installableApps.wbm\samples\  
mortgageLending\
```

Das Modell heißt `MortgageLendingBAMApplication.ear`.

Wenn Sie ein eigenständiges Profil erstellt haben, können Sie eine der folgenden Methoden verwenden.

- (Nicht für z/OS:) Installieren Sie das Präsentationsmodell mit 'Erste Schritte'.
  1. Wählen Sie für den Zugriff auf 'Erste Schritte' über das eigenständige Profil eine der folgenden Optionen aus:
    - Wählen Sie in der Anzeige **Profilerstellung abgeschlossen** die Option **IBM Business Monitor-Erste Schritte starten** aus.
    - Rufen Sie **Start > Alle Programme > IBM > Business Monitor 8.0 > Profile > profilname > Erste Schritte** auf.
    - Wechseln Sie zu `profil-stammverzeichnis\firststeps.wbm` und führen Sie den Befehl `firststeps.bat` aus.

**Wichtig:** Um die Einführung (First Steps) unter Windows 7, Windows Vista oder Windows Server 2008 zu installieren, müssen Sie die Rechte Ihres Microsoft Windows Benutzeraccounts erweitern, indem Sie mit der rechten Maustaste auf `firststeps.bat` klicken und **Run as administrator** (Als Administrator ausführen) auswählen. Dies ist sowohl für Administratoren als auch für Benutzer ohne Administratorrechte erforderlich.

- Öffnen Sie ein Befehlsfenster. Wechseln Sie in das Verzeichnis `profil-stammverzeichnis/firststeps.wbm` und führen Sie den Befehl `firststeps.sh` aus.
- 2. Wählen Sie in der Konsole 'Erste Schritte' die Option **Präsentationsmodell** aus.

**Anmerkung:** Bei aktivierter Sicherheit werden Sie zur Eingabe einer WebSphere Application Server-Benutzer-ID und des zugehörigen Kennworts aufgefordert.

- Installieren Sie das Präsentationsmodell mit der Administrationskonsole. Klicken Sie auf **Anwendungen > Monitormodelle**. Klicken Sie auf **Installieren** und wäh-

len Sie die Datei MortgageLendingBAMApplication.ear aus. Verwenden Sie die Standardeinstellungen für die Installation.

Starten Sie nach Abschluss der Installation den Server erneut und öffnen Sie Business Space, um den Space 'Better Lender' anzuzeigen. (Die Konsole 'Erste Schritte' enthält sowohl eine Option zum Starten des Servers als auch eine Option zum Starten von Business Space.)

---

## Kapitel 12. IBM Business Monitor aktualisieren

Sie können Aktualisierungen für IBM Business Monitor installieren, sobald diese verfügbar sind.

Auf der IBM Support-Website können Sie prüfen, ob Fixpacks und vorläufige Fixes verfügbar sind.

---

### IBM Cognos BI aktualisieren



Wenn Sie IBM Cognos Business Intelligence oder Ihre JDBC-Treiber (Java Database Connectivity) aktualisieren, müssen Sie auch die IBM Cognos BI-EAR-Datei (Enterprise Archive) neu generieren. Die implementierte IBM Cognos BI-Serviceanwendung muss mit der neuen EAR-Datei aktualisiert werden.

Alle Knoten, auf denen die IBM Cognos BI-Serviceanwendung ausgeführt wird, müssen dieselbe Version und denselben Service-Level von IBM Cognos BI ausführen.

**Wichtig:** Aktualisieren Sie nur die Basisverzeichnisse von IBM Cognos BI (die Verzeichnisse unter dem WebSphere-Stammverzeichnis). Die kopierten Laufzeitinstanzen (die Verzeichnisse unter dem Profil) werden von IBM Business Monitor beim nächsten Start des IBM Cognos BI-Servers aktualisiert.

Führen Sie folgende Schritte aus, um IBM Cognos BI und die EAR-Datei zu aktualisieren:

1. Gehen Sie wie folgt vor, um IBM Cognos BI zu aktualisieren:
  - a. Fordern Sie die komprimierte Datei (tar.gz) für den IBM Cognos BI-Service für den Plattformtyp Ihres Knotens an.
  - b. Entpacken Sie die Datei in einem Arbeitsverzeichnis.
  - c. Suchen Sie den Befehl **issetup** und führen Sie ihn aus. Wenn Sie zur Eingabe der Installationsposition aufgefordert werden, geben Sie `application_server-stammverzeichnis/cognos` ein.

**Tipp:**   Wenn Sie die grafische Benutzerschnittstelle der Aktualisierung nicht ausführen können oder wenn Sie wissen, dass das MO-TIF-Paket nicht installiert ist, müssen Sie das Programm für die unbeaufsichtigte Installation aus Ihrer bestehenden IBM Cognos BI-Installation kopieren. Führen Sie die folgenden Schritte aus:

- 1) Suchen Sie die Datei in Ihrer IBM Cognos BI-Installation:  
`application_server-stammverzeichnis/cognos/uninstall/issetupnx`
- 2) Kopieren Sie die Datei in das Arbeitsverzeichnis des neuen Installationsprogramms und stellen Sie sie in dasselbe Verzeichnis wie **issetup**.
- 3) Aktualisieren Sie die Datei `response.ats` und fügen Sie ihr die folgenden Werte hinzu:

```
I Agree=y
APPDIR=application_server-stammverzeichnis/cognos
C8BISRVR_APP=1
C8BISRVR_APPLICATION_TIER=1
C8BISRVR_GATEWAY=1
C8BISRVR_CONTENT_MANAGER=1
C8BISRVR_CONTENT_DATABASE=1
```

- 4) Öffnen Sie eine Eingabeaufforderung im Arbeitsverzeichnis und führen Sie den folgenden Befehl aus:
 

```
./issetupnx -s
```
2. Führen Sie folgende Schritte aus, um nach der Aktualisierung von IBM Cognos BI die EAR-Datei zu aktualisieren:
  - a. Wenn Sie Ihre JDBC-Treiber aktualisiert haben, müssen Sie die neue Version sowohl auf IBM Cognos Business Intelligence als auch auf IBM Business Monitor anwenden. Vor der Neugenerierung der EAR-Datei wenden Sie die neue Version auf IBM Cognos BI in den folgenden Verzeichnissen an:
 

```
application_server-stammverzeichnis/cognos/webapps/p2pd/WEB-INF/lib
application_server-stammverzeichnis/cognos/v5dataserver/lib
```
  - b. Auf Ihrem Deployment Manager oder eigenständigen Server öffnen Sie eine Eingabeaufforderung in `application_server-stammverzeichnis/cognos/war/p2pd`.
  - c. Führen Sie den folgenden Befehl aus:
 

```
Windows build.bat ear
Linux UNIX build.sh ear
```

Mit diesem Befehl wird eine WebSphere-EAR-Datei mit dem Namen `p2pd.ear` im IBM Cognos BI-Stammverzeichnis erstellt. Die Erstellung der EAR-Datei kann einige Minuten in Anspruch nehmen.
  - d. Öffnen Sie auf Ihrem Deployment Manager oder eigenständigen Server die WebSphere-Administrationskonsole und klicken Sie auf **Anwendungen** > **Anwendungstyp** > **WebSphere-Unternehmensanwendungen**.
  - e. Wählen Sie das Kontrollkästchen **IBM Cognos** aus und klicken Sie auf **Aktualisieren**.
  - f. Suchen Sie unter **Pfad zur EAR-Ersatzdatei angeben** nach der EAR-Datei, die Sie in Schritt c erstellt haben.
  - g. Führen Sie die Schritte im Aktualisierungsassistenten durch, um die Anwendung zu aktualisieren. Nach dem Klicken auf **Fertig stellen** kann die Aktualisierung einige Minuten in Anspruch nehmen.
  - h. Speichern Sie Ihre Änderungen. Die Speicherung der neuen Konfiguration kann einige Minuten dauern.
  - i. Starten Sie die Anwendungsserver erneut, die mit der neuen IBM Cognos BI-EAR-Datei aktualisiert wurden.

---

## Fixpacks und vorläufige Fixes im Dialogbetrieb installieren

Mit IBM Installation Manager können Sie im Dialogbetrieb Aktualisierungen für Softwarepakete installieren.

Sie können mithilfe dieser Prozedur nicht Aktualisierungen für die zugrunde liegende Instanz von IBM DB2 Express oder IBM Cognos BI installieren. Sie müssen die Produkte gemäß den normalen Aktualisierungsprozessen aktualisieren.

Auf der IBM Support-Website können Sie prüfen, ob Fixpacks und vorläufige Fixes verfügbar sind.

Führen Sie vor der Installation eines Fixpacks oder vorläufigen Fixes die folgenden Tasks aus:

1. Lesen Sie die Dokumentation des Fixpacks bzw. des vorläufigen Fixes sorgfältig durch. In der Dokumentation sind Abhängigkeiten aufgeführt. Hierzu können

Fixpackstufen von WebSphere Application Server oder Fixes für andere IBM Produkte gehören, die vor dem Anwenden des Fixpacks oder des vorläufigen Fixes installiert werden müssen.

2. Bereiten Sie einen Regressionstestplan vor, um zu gewährleisten, dass Ihre Implementierung genauso wie vor dem Anwenden des Fixpacks oder des vorläufigen Fixes funktioniert.
3. Sichern Sie die Datenbank und das Profil.
4. Installieren Sie das Fixpack bzw. den vorläufigen Fix in einer Entwicklungs- oder Qualitätssicherungsumgebung, bevor Sie die Implementierung in einer Produktionsumgebung vornehmen.
5. Zur Installation müssen Sie dasselbe Benutzerkonto verwenden, mit dem Sie auch die Produktpakete installiert haben.

In jedes installierte Paket ist die Position seines IBM Standard-Update-Repositorys integriert. Damit Installation Manager die Positionen des IBM Aktualisierungsrepositorys nach den installierten Paketen durchsucht, muss auf der Seite mit den Benutzervorgaben für Repositorys die Einstellung **Die Service-Repositorys während Installation und Aktualisierungen durchsuchen** aktiviert sein. Diese Einstellung ist standardmäßig aktiviert.

Während des Aktualisierungsprozesses fordert Installation Manager Sie möglicherweise auf, die Position des Repositorys für die Basisversion des Pakets anzugeben. Wenn Sie das Produkt von DVDs oder von anderen Datenträgern installiert haben, müssen diese bei Verwendung der Aktualisierungsfunktion verfügbar sein.

Weitere Informationen zu Installation Manager erhalten Sie nach Auswahl des Links zum Information Center, der im Abschnitt mit den Referenzinformationen verfügbar ist.

**Wichtig:** Alle vorhandenen Profile bleiben erhalten und müssen nicht erneut erstellt werden.

Gehen Sie wie folgt vor, um nach Paketaktualisierungen zu suchen und diese zu installieren:

1. Stoppen Sie die gesamte Software für das Produkt, das Sie aktualisieren wollen. Schließen Sie Programme und stoppen Sie Server, die Profile für dieses Produkt enthalten.
2. Starten Sie Installation Manager. Klicken Sie auf der Startseite von Installation Manager auf **Aktualisieren**.

 Sie können auch auf **Start > Programme > IBM > paketgruppenname > Aktualisieren** klicken. Klicken Sie zum Beispiel auf **Start > Programme > IBM > IBM Business Monitor > Aktualisieren**.

3. Wenn IBM Installation Manager auf Ihrem System nicht vorhanden ist oder wenn bereits eine ältere Version installiert ist, müssen Sie mit der Installation des aktuellsten Release fortfahren. Folgen Sie den angezeigten Anweisungen des Assistenten, um die Installation von IBM Installation Manager abzuschließen.
4. Wenn Sie nicht über einen Internetzugang verfügen, laden Sie den vorläufigen Fix oder das Fixpack lokal herunter, extrahieren Sie ihn/es in einem eigenen Verzeichnis und fügen Sie das neue Verzeichnis zu Installation Manager hinzu.
  - a. Starten Sie Installation Manager.

- b. Klicken Sie auf der Startseite auf **Datei > Benutzervorgaben > Repositories**.
  - c. Klicken Sie auf der Seite 'Repositories' auf **Repository hinzufügen**.
  - d. Wählen Sie im Fenster **Repository hinzufügen** das neue Verzeichnis aus, in dem sich die extrahierten Dateien für den vorläufigen Fix bzw. das Fixpack befinden.
  - e. Wählen Sie die Datei `repository.config` aus und klicken Sie auf **Öffnen**.
  - f. Klicken Sie auf der Seite 'Repositories' auf **OK**.
5. Wählen Sie im Assistenten 'Pakete aktualisieren' die Paketgruppe aus, die das zu aktualisierende Produktpaket enthält, oder wählen Sie das Kontrollkästchen **Alle aktualisieren** aus. Klicken Sie anschließend auf **Weiter**. Installation Manager sucht in seinen Repositories und den vordefinierten Update-Sites nach der Software, die aktualisiert werden soll. Ein Statusanzeiger zeigt den Fortschritt der laufenden Suche an.
  6. Wenn für ein Paket Aktualisierungen gefunden werden, werden diese in der Liste **Aktualisierungen** auf der Seite 'Aktualisierungspakete' unter dem entsprechenden Paket angezeigt. Standardmäßig werden nur die neuesten empfohlenen Aktualisierungen angezeigt. Klicken Sie auf **Alle anzeigen**, damit alle Aktualisierungen angezeigt werden, die für die verfügbaren Pakete gefunden wurden.
    - a. Klicken Sie auf eine Aktualisierung und lesen Sie die unter **Details** angezeigte Beschreibung, wenn Sie sich näher über eine Aktualisierung informieren möchten.
    - b. Wenn zusätzliche Informationen zu der Aktualisierung verfügbar sind, ist unter dem Beschreibungstext der Link **Weitere Informationen** vorhanden. Klicken Sie auf den Link, um die Informationen in einem Browser anzuzeigen. Prüfen Sie diese Informationen, bevor Sie die Aktualisierung installieren.
  7. Wählen Sie die Aktualisierungen aus, die Sie installieren möchten, oder klicken Sie auf **Empfohlene auswählen**, um die Auswahl der Standardoptionen wieder herzustellen. Klicken Sie anschließend auf **Weiter**. Aktualisierungen, die eine Abhängigkeitsbeziehung aufweisen, werden automatisch gemeinsam aus- und abgewählt.
  8. Lesen Sie auf der Seite **Lizenzen** die Lizenzvereinbarungen für die ausgewählten Aktualisierungen. Im linken Teil der Seite 'Lizenzen' wird die Liste der Lizenzen für die von Ihnen ausgewählten Aktualisierungen angezeigt. Klicken Sie auf die einzelnen Elemente, um den jeweiligen Lizenzvereinbarungstext anzuzeigen. Wenn Sie den Bedingungen der Lizenzvereinbarung zustimmen, klicken Sie auf **Ich akzeptiere die Bedingungen der Lizenzvereinbarungen**. Klicken Sie anschließend auf **Weiter**. Wenn Sie die Bedingungen der Lizenzvereinbarung nicht akzeptieren, kann das Fixpack oder der vorläufige Fix nicht installiert werden.
  9. Überprüfen Sie Ihre Auswahl auf der Seite **Zusammenfassung**, bevor Sie die Aktualisierungen installieren.
    - a. Wenn Sie Ihre Auswahl auf der vorherigen Seite ändern möchten, klicken Sie auf **Zurück** und nehmen Sie die Änderungen vor.
    - b. Wenn die Auswahl Ihren Wünschen entspricht, klicken Sie auf **Aktualisieren**, um die Aktualisierungen herunterzuladen und zu installieren. Ein Statusanzeiger zeigt an, zu welchem Prozentsatz die Installation abgeschlossen ist.
  10. Optional: Wenn der Aktualisierungsprozess abgeschlossen ist, wird im oberen Bereich der Seite eine Nachricht mit der Bestätigung angezeigt, dass der Pro-



zess erfolgreich ausgeführt wurde. Klicken Sie auf **Protokolldatei anzeigen**, um die Protokolldatei für die aktuelle Sitzung in einem neuen Fenster zu öffnen. Sie müssen das Fenster mit dem Installationsprotokoll schließen, um fortfahren zu können.

11. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.
12. Schließen Sie Installation Manager.

---

## Fixpacks unbeaufsichtigt installieren

Sie können Fixpacks für IBM Business Monitor unbeaufsichtigt installieren.

Auf der IBM Support-Website können Sie prüfen, ob Fixpacks und vorläufige Fixes verfügbar sind.

Führen Sie vor der Installation eines Fixpacks die folgenden Tasks aus:

1. Lesen Sie die Dokumentation des Fixpacks sorgfältig durch. In der Dokumentation sind Abhängigkeiten aufgeführt. Hierzu können Fixpackstufen von WebSphere Application Server oder Fixes für andere IBM Produkte gehören, die vor dem Anwenden des Fixpacks installiert werden müssen.
2. Bereiten Sie einen Regressionstestplan vor, um zu gewährleisten, dass Ihre Implementierung genauso wie vor dem Anwenden des Fixpacks funktioniert.
3. Sichern Sie die Datenbank und das Profil.
4. Installieren Sie das Fixpack in einer Entwicklungs- oder Qualitätssicherungsumgebung, bevor Sie die Implementierung in einer Produktionsumgebung vornehmen.
5. Zur Installation müssen Sie dasselbe Benutzerkonto verwenden, mit dem Sie auch die Produktpakete installiert haben.

Sie können mithilfe dieser Prozedur nicht Aktualisierungen für die zugrunde liegende Instanz von IBM DB2 Express oder IBM Cognos BI installieren. Sie müssen die Produkte gemäß den normalen Aktualisierungsprozessen aktualisieren.

Gehen Sie wie folgt vor, um ein Fixpack zu IBM Business Monitor hinzuzufügen:

1. Lesen Sie die Lizenzbedingungen, bevor Sie die Aktualisierung ausführen. Wenn Sie den Parameter `-acceptLicense` zur Befehlszeile hinzufügen, akzeptieren Sie alle Lizenzbedingungen. Wenn Sie die Lizenz nicht akzeptieren, kann die Installation nicht ausgeführt werden.
2. Führen Sie den folgenden Befehl aus:

**Wichtig:** Wenn Sie Windows 7, Windows Vista oder Windows Server 2008 verwenden, starten Sie die Eingabeaufforderung, indem Sie mit der rechten Maustaste klicken und die Option **Als Administrator ausführen** auswählen.

 Windows

```
extraktionsverzeichnis\IM\tools\imcl install liste_der_produk-IDs -acceptLicense -installatio
```

 UNIX  Linux

```
extraktionsverzeichnis/IM/tools/imcl install liste_der_produk-IDs -acceptLicense -installatio
```

Hierbei gilt Folgendes:

- `liste_der_produk-IDs` ist eine Liste der IDs für die Produkte (durch Kommas getrennt), die Sie aktualisieren möchten.

Tabelle 8. Produkt-IDs

| Produkt                                         | Produkt-ID                    |
|-------------------------------------------------|-------------------------------|
| IBM Business Monitor                            | com.ibm.websphere.MON.V80     |
| IBM Business Monitor for z/OS                   | com.ibm.websphere.ZOS.MON.V80 |
| WebSphere Application Server Network Deployment | com.ibm.websphere.ND.v80      |
| WebSphere Application Base                      | com.ibm.websphere.BASE.v80    |

- *extraktionsverzeichnis* ist der Pfad, in dem Sie die Fixpackdateien extrahiert haben.
- *position* ist der Pfad zu dem Verzeichnis, in dem Sie die Produkte aktualisieren möchten.
- *repository* ist der Pfad zu dem Repository, in dem Sie die Fixpackdateien extrahiert haben. Mehrere Repositories können Sie angeben, indem Sie die Repository-Positionen durch Kommas voneinander abgrenzen.
- *protokollname* ist der Name der Protokolldatei zur Aufzeichnung von Nachrichten und Ergebnissen.

Installation Manager aktualisiert die in der Liste aufgeführten Produkte und schreibt eine Protokolldatei in das von Ihnen angegebene Verzeichnis.

Im folgenden Beispiel wird IBM Business Monitor unter Windows aktualisiert.

```
imcl install com.ibm.websphere.MON.V80 com.ibm.websphere.ND.v80 -acceptLicense -installationDirectory
```

---

## Vorläufige Fixes unbeaufsichtigt installieren

Sie können einen vorläufigen Fix für IBM Business Monitor im Befehlszeilenmodus von Installation Manager installieren.

Auf der IBM Support-Website können Sie prüfen, ob Fixpacks und vorläufige Fixes verfügbar sind.

Führen Sie vor der Installation eines vorläufigen Fixes die folgenden Tasks aus:

1. Lesen Sie die Dokumentation des vorläufigen Fixes sorgfältig durch. In der Dokumentation sind Abhängigkeiten aufgeführt. Hierzu können Fixpackstufen von WebSphere Application Server oder Fixes für andere IBM Produkte gehören, die vor dem Anwenden des vorläufigen Fixes installiert werden müssen.
2. Bereiten Sie einen Regressionstestplan vor, um zu gewährleisten, dass Ihre Implementierung genauso wie vor dem Anwenden des vorläufigen Fixes funktioniert.
3. Sichern Sie die Datenbank und das Profil.
4. Installieren Sie den vorläufigen Fix in einer Entwicklungs- oder Qualitätssicherungsumgebung, bevor Sie ihn in einer Produktionsumgebung implementieren.
5. Zur Installation müssen Sie dasselbe Benutzerkonto verwenden, mit dem Sie auch die Produktpakete installiert haben.

Bei dieser Prozedur wird der vorläufige Fix in einem lokalen Verzeichnis gespeichert. Informationen zur Verwendung eines Online-Repositorys als Speicherort für vorläufige Fixdateien und andere Konfigurationsdaten finden Sie im Information Center von IBM Installation Manager.

Gehen Sie zur unbeaufsichtigten Installation des vorläufigen Fixes folgendermaßen vor:

1. Laden Sie den vorläufigen Fix auf das lokale System herunter.
2. Erstellen Sie ein neues Verzeichnis und extrahieren Sie den vorläufigen Fix in das neue Verzeichnis.
3. Öffnen Sie eine Eingabeaufforderung und wechseln Sie in das Verzeichnis `/eclipse/tools` unter Installation Manager.

**Wichtig:** Wenn Sie Windows 7, Windows Vista oder Windows Server 2008 verwenden, starten Sie die Eingabeaufforderung, indem Sie mit der rechten Maustaste klicken und die Option **Als Administrator ausführen** auswählen.

4. Nehmen Sie die erforderlichen Ersetzungen vor und führen Sie den folgenden Befehl aus:

```
imcl install fixID -repositories repositoryLocation -installationDirectory installationDirectory
```

- a. Ersetzen Sie *fixID* durch die ID des vorläufigen Fixes. Die ID finden Sie in der Datei `repository.xml` in dem Verzeichnis, in dem Sie den vorläufigen Fix extrahiert haben, im Element `fix id`. Beispiel:

```
<fix id="8.0.0.0-WS-BPMADVWESB-IFJR39658" version="0.0.0.20111115_1047" offeringId="Enhance
```

- b. Ersetzen Sie *repositoryLocation* durch das Verzeichnis, in das Sie den vorläufigen Fix extrahiert haben.
- c. Ersetzen Sie *installationDirectory* durch die Position, an der Sie IBM Business Monitor installiert haben.
- d. Ersetzen Sie *logLocation* durch die Position und den Dateinamen für das Protokoll für die Installationsinformationen.

Beispiel:

```
C:\Program Files\IBM\Installation Manager\eclipse\tools>imcl install 8.0.0.0-WS-BPMADVWESB-IFJ  
C:\interimFix\8.0.0.0-WS-BPMADVWESB-IFJR39658/ -installationDirectory C:\IBM\BPM80 -log log
```

Bei erfolgreicher Installation des vorläufigen Fixes enthält das Installationsprotokoll (wie im Parameter **-log** angegeben) keine Fehlermeldungen. In der Befehlszeile wird eine Nachricht angezeigt, aus der hervorgeht, dass der Fix installiert wurde.

Beispiel:

```
Installed 8.0.0.0-WS-BPMADVWESB-IFJR39658_0.0.0.20110525_1047 to the C:\IBM\BPM80 directory.
```

---

## Rollback eines Fixpacks durchführen

Mit dem Assistenten zum Durchführen von Rollbacks für Pakete können Sie ein Fixpack für die IBM Business Monitor-Installation rückgängig machen und zu einer Vorgängerversion zurückkehren.

Während des Rollbackprozesses muss Installation Manager auf Dateien aus der Vorgängerversion des Pakets zugreifen. Diese Dateien werden beim Installieren eines Pakets standardmäßig auf Ihrem System gespeichert. Wenn die Dateien nicht auf Ihrer Workstation verfügbar sind, müssen Sie auch die Position des Repositories, von dem aus Sie die Vorgängerversion des Produkts installiert haben, in den Benutzervorgaben für Installation Manager (**Datei > Benutzervorgaben > Repository**) angeben. Wenn Sie das Produkt von DVDs oder von anderen Datenträgern installiert haben, müssen diese bei Verwendung der Rollbackfunktion verfügbar sein.

Sie können die Rollbackfunktion verwenden, wenn Sie ein Fixpack auf ein Produktpaket angewendet haben und diese Aktualisierung zu einem späteren Zeitpunkt entfernen und zur ursprünglichen Version des Produkts zurückkehren

möchten. Bei Verwendung der Rollbackfunktion deinstalliert Installation Manager die aktualisierten Ressourcen und installiert wieder die Ressourcen der Vorgängerversion.

Wenn Sie ein Rollback auf eine frühere Version eines Pakets durchführen, wird diese mit den Features wiederhergestellt, die dieser Version zugeordnet waren. Mit dem Assistenten 'Pakete ändern' können Sie Features hinzufügen und entfernen.

Weitere Informationen zu Installation Manager (unter anderem Anweisungen für die Durchführung eines Rollbacks über die Befehlszeile) finden Sie im Information Center von Installation Manager.

1. Stoppen Sie die gesamte Software für das Produkt, für das Sie ein Rollback durchführen wollen. Schließen Sie Programme und stoppen Sie Server, die Profile für dieses Produkt enthalten.
2. Starten Sie Installation Manager.
3. Klicken Sie auf der Startseite von Installation Manager auf die Option **Rollback durchführen**, um den Assistenten für das Rollback von Paketen zu starten.
4. Wählen Sie auf der Seite 'Rollback für Pakete durchführen' in der Liste der Paketgruppennamen die Paketgruppe aus, die das Paket enthält, für das Sie ein Rollback ausführen wollen. Klicken Sie anschließend auf **Weiter**.
5. Wählen Sie die Version des Pakets aus, für die das Rollback ausgeführt werden soll, und klicken Sie auf **Weiter**.
6. Lesen Sie die Informationen der Zusammenfassung und klicken Sie auf **Rollback durchführen**, um das Rollback für das Paket durchzuführen.
7. Optional: Wenn der Rollbackprozess abgeschlossen ist, wird im oberen Bereich der Seite eine Nachricht mit der Bestätigung angezeigt, dass der Prozess erfolgreich ausgeführt wurde. Klicken Sie auf **Protokolldatei anzeigen**, um die Protokolldatei für die aktuelle Sitzung in einem neuen Fenster zu öffnen.
8. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.
9. Schließen Sie Installation Manager.

Das Fixpack, für das Sie eine Rollback-Operation ausgewählt haben, wurde entfernt.

---

## Vorläufige Fixes im Dialogbetrieb deinstallieren

Mithilfe von Installation Manager können Sie einen oder mehrere vorläufige Fixes für IBM Business Monitor deinstallieren.

Zur Deinstallation müssen Sie dasselbe Benutzerkonto verwenden, mit dem Sie die Produktpakete auch installiert haben.

**Wichtig:** Ein vorläufiger Fix kann nicht deinstalliert werden, wenn ein anderer vorläufiger Fix eine Abhängigkeit zu ihm aufweist, sofern nicht der abhängige vorläufige Fix ebenfalls zur Deinstallation ausgewählt wird. Wenn Sie versuchen, einen vorläufigen Fix zu entfernen, von dem ein anderer vorläufiger Fix abhängig ist, empfangen Sie eine Fehlermeldung.

Gehen Sie folgendermaßen vor, um einen vorläufigen Fix im Dialogbetrieb zu deinstallieren:

1. Stoppen Sie die gesamte Software für das Produkt, das Sie aktualisieren wollen. Schließen Sie Programme und stoppen Sie Server, die Profile für dieses Produkt enthalten.

2. Starten Sie Installation Manager. Klicken Sie auf der Startseite auf **Deinstallieren**.
3. Wählen Sie auf der Seite 'Pakete deinstallieren' einen oder mehrere vorläufige Fixes für die Deinstallation aus und klicken Sie auf **Weiter**.
4. Prüfen Sie Ihre Auswahl auf der Seite 'Zusammenfassung' und klicken Sie anschließend auf **Deinstallieren**. Nach Abschluss der Deinstallation wird die Seite 'Fertig' geöffnet.
5. Klicken Sie auf **Fertig stellen**, um den Assistenten zu verlassen.

Die Deinstallation des/der vorläufigen Fixes ist hiermit abgeschlossen.

**Wichtig:** Löschen Sie nach der Deinstallation von vorläufigen Fixes auf keinen Fall das Eclipse-Konfigurationsverzeichnis. Das Löschen dieser Informationen wirkt sich nachteilig auf den Betrieb von Installation Manager aus. Standardmäßig handelt es sich hierbei um das Verzeichnis `configuration` im `installationsstammverzeichnis`.

---

## Vorläufige Fixes unbeaufsichtigt deinstallieren

Deinstallieren Sie einen vorläufigen Fix für IBM Business Monitor im Befehlszeilenmodus von Installation Manager.

Zur Deinstallation müssen Sie dasselbe Benutzerkonto verwenden, mit dem Sie die Produktpakete auch installiert haben.

**Wichtig:** Ein vorläufiger Fix kann nicht deinstalliert werden, wenn ein anderer vorläufiger Fix eine Abhängigkeit zu ihm aufweist, sofern nicht der abhängige vorläufige Fix ebenfalls zur Deinstallation ausgewählt wird. Wenn Sie versuchen, einen vorläufigen Fix zu entfernen, von dem ein anderer vorläufiger Fix abhängig ist, empfangen Sie eine Fehlermeldung.

Gehen Sie zur unbeaufsichtigten Deinstallation eines vorläufigen Fixes folgendermaßen vor:

1. Stoppen Sie die gesamte Software für das Produkt, das Sie aktualisieren wollen. Schließen Sie Programme und stoppen Sie Server, die Profile für dieses Produkt enthalten.
2. Öffnen Sie eine Eingabeaufforderung und wechseln Sie in das Verzeichnis `/eclipse/tools` unter Installation Manager.

**Wichtig:** Wenn Sie Windows 7, Windows Vista oder Windows Server 2008 verwenden, starten Sie die Eingabeaufforderung, indem Sie mit der rechten Maustaste klicken und die Option **Als Administrator ausführen** auswählen.

3. Nehmen Sie die erforderlichen Ersetzungen vor und führen Sie den folgenden Befehl aus:

```
imcl uninstall fixID -installationDirectory installationsverzeichnis -log protokollposition
```

- a. Ersetzen Sie *fixID* durch die ID des vorläufigen Fixes. Die ID finden Sie in der Datei `repository.xml` in dem Verzeichnis, in dem Sie den vorläufigen Fix extrahiert haben, im Element `fix id`. Beispiel:

```
<fix id="8.0.0.0-WS-BPMADVWESB-IFJR39658" version="0.0.0.20111115_1047" offeringId="Enhance
```

- b. Ersetzen Sie *installationsverzeichnis* durch die Position, an der Sie IBM Business Monitor installiert haben.
- c. Ersetzen Sie *protokollposition* durch die Position und den Namen der Datei, in der die Informationen protokolliert werden sollen.

Beispiel:

```
C:\Program Files\IBM\Installation Manager\eclipse\tools>imcl uninstall 8.0.0.0-WS-BPMADVWESB-IFJR
```

Bei erfolgreicher Deinstallation enthält das Protokoll (wie im Parameter **-log** angegeben) keine Fehlermeldungen. In der Befehlszeile wird eine Nachricht angezeigt, aus der hervorgeht, dass der Fix deinstalliert wurde.



---

## Kapitel 13. IBM Business Monitor deinstallieren

Sie können IBM Business Monitor im Dialogbetrieb oder im unbeaufsichtigten Modus deinstallieren.


---

### IBM Business Monitor interaktiv deinstallieren

Die Deinstallationsoption in Installation Manager ermöglicht das Deinstallieren von Paketen aus einem einzelnen Installationsverzeichnis. Sie können auch alle installierten Pakete aus sämtlichen Installationsverzeichnissen deinstallieren.

Zum Deinstallieren der Pakete müssen Sie sich beim System mit demselben Benutzerkonto anmelden, das Sie auch für die Installation der Produktpakete verwendet haben. Ein Paket kann nicht deinstalliert werden, wenn ein anderes Paket eine Abhängigkeit zu ihm aufweist, sofern nicht das abhängige Paket ebenfalls zur Deinstallation ausgewählt wird.

1. Schließen Sie die Programme, die mit Installation Manager installiert wurden.
2. Stoppen Sie alle aktiven Server.
3. Rufen Sie die Seite **Pakete deinstallieren** von Installation Manager auf.
  - Starten Sie Installation Manager. Klicken Sie auf der Startseite auf **Deinstallieren**.
4. Wählen Sie auf der Seite 'Pakete deinstallieren' IBM Business Monitor und zugehörige Pakete aus, die Sie deinstallieren wollen.

**Tipp:**  Falls Sie Installation Manager im vorherigen Schritt über das Menü 'Start' aufgerufen haben (**Start > ... > Deinstallieren**), ist Ihre IBM Business Monitor Edition auf der Seite **Pakete deinstallieren** bereits für die Deinstallation ausgewählt.

Wenn Sie DB2 Express nicht mehr benötigen oder IBM Business Monitor erneut installieren wollen, wählen Sie die Option **IBM DB2 Express** aus, um DB2 Express zu deinstallieren. **Vorsicht:**


**Wählen Sie die Option für die Deinstallation von DB2 Express nur dann aus, wenn Sie sicher sind, dass DB2 Express von keinem anderen Produkt verwendet wird. Bei Auswahl dieser Option werden alle DB2 Express-Datenbanken und -Datenbankassets selbst dann gelöscht, wenn andere Produkte (dies schließt auch Produkte auf einem fernen System ein) möglicherweise DB2 Express auf diesem System verwenden.**

5. Klicken Sie auf **Weiter**.
6. Überprüfen Sie auf der Seite 'Zusammenfassung' die Liste der zu deinstallierenden Pakete und klicken Sie anschließend auf **Deinstallieren**. Nach Abschluss der Deinstallation wird die Seite **Fertig** geöffnet.
7. Klicken Sie auf **Fertig stellen**, um den Assistenten zu verlassen.

Bei der Deinstallation von IBM Business Monitor werden alle Profile, die für IBM Business Monitor erweitert wurden, entfernt, einschließlich aller WebSphere Application Server-Profilen, die für IBM Business Monitor erweitert wurden. Bei eigenständigen Monitor-Server-Profilen wird der IBM Cognos BI-Service entfernt.

Beispiel-Monitor-Modelle werden nicht deinstalliert, um sicherzustellen, dass Anpassungen der Modelle erhalten bleiben. Informationen zur Deinstallation dieser Modelle finden Sie unter Entfernen von Monitor-Modellen und Monitor-Daten.

Wenn Sie beabsichtigen, IBM Business Monitor erneut zu installieren, prüfen Sie mögliche Datenbankprobleme, die sich auf das Neuinstallationsverfahren auswirken könnten. Führen Sie alle gegebenenfalls erforderlichen Aktionen aus, bevor Sie das Produkt erneut installieren:

- Falls bei der vorherigen Installation Datenbanken erstellt wurden, müssen Sie sicherstellen, dass die Datenbanken gelöscht werden (siehe Neuinstallation kann kein neues Profil erstellen).
- Falls Sie DB2 Express deinstalliert haben, müssen Sie sicherstellen, dass das Verzeichnis BPMINST gelöscht wurde
-  Falls Sie DB2 Express deinstalliert haben, müssen Sie die verbleibenden Einträge für DB2 Express in der Datei /etc/service löschen. Dies ist erforderlich, weil die Neuinstallation voraussetzt, dass der Port 50000 verfügbar ist. Suchen und entfernen Sie in der Datei /etc/service alle Verweise auf DB2 Express und Port 50000. Beispiele:

```
db2c_bpminst 50000/tcp
```

oder

```
db2c_db2inst1 50000/tcp
```

---

## IBM Business Monitor unbeaufsichtigt deinstallieren

Verwenden Sie zur Deinstallation von IBM Business Monitor den Befehlszeilenmodus von Installation Manager.

Schließen Sie sämtliche Programme, die mit Installation Manager installiert wurden.

Um eine Deinstallation vorzunehmen, müssen Sie sich mit demselben Benutzeraccount wie bei der Installation der Produktpakete beim System anmelden.

Gehen Sie wie folgt vor, um IBM Business Monitor im unbeaufsichtigten Modus zu deinstallieren:

1. Öffnen Sie eine Eingabeaufforderung und wechseln Sie in das Verzeichnis `/eclipse/tools` unter Installation Manager.

**Wichtig:** Wenn Sie das Betriebssystem Windows 7, Windows Vista oder Windows Server 2008 verwenden, starten Sie die Eingabeaufforderung durch Klicken mit der rechten Maustaste und Auswählen von **Run as administrator** (Als Administrator ausführen).

2. Nehmen Sie die entsprechenden Ersetzungen vor und führen Sie den folgenden Befehl aus:

```
imcl uninstall liste_von_produkts-IDs -installationDirectory installationsverzeichnis -log protokoll
```

- a. Ersetzen Sie die `liste_der_produkts_IDS` durch eine Liste von, durch Leerzeichen getrennte IDs derjenigen Produkte, die Sie deinstallieren möchten.

**Wichtig:** Die Installation von DB2 Express kann von verschiedenen Produkten verwendet werden. Dies schließt auch Produkte auf einem fernen System ein. Falls Sie DB2 Express deinstallieren, werden alle DB2 Express-Datenbanken und -Datenbankassets gelöscht.

Tabelle 9. Produkt-IDs

| Produkt                                                   | Produkt-ID                        |
|-----------------------------------------------------------|-----------------------------------|
| IBM Business Monitor                                      | com.ibm.websphere.MON.V80         |
| WebSphere Application Server Network Deployment           | com.ibm.websphere.ND.v80          |
| Installation Manager                                      | com.ibm.cic.agent                 |
| DB2 for Linux 32-bit                                      | com.ibm.ws.DB2EXP97.linuxia32     |
| DB2 for Linux 64-bit                                      | com.ibm.ws.DB2EXP97.linuxia64     |
| DB2 for Windows 32-bit                                    | com.ibm.ws.DB2EXP97.winia32       |
| DB2 for Windows 64-bit                                    | com.ibm.ws.DB2EXP97.winia64       |
| IBM Cognos Business Intelligence for Windows x86 (32-Bit) | com.ibm.ws.cognos.v1011.winia32   |
| IBM Cognos BI for Windows x64 (64-Bit)                    | com.ibm.ws.cognos.v1011.winia64   |
| IBM Cognos BI for AIX PPC 32-Bit                          | com.ibm.ws.cognos.v1011.aix32     |
| IBM Cognos BI for AIX PPC 64-Bit                          | com.ibm.ws.cognos.v1011.aix64     |
| IBM Cognos BI for Linux x86 (32-Bit)                      | com.ibm.ws.cognos.v1011.linuxia32 |
| IBM Cognos BI for Linux x86-64 (64-Bit)                   | com.ibm.ws.cognos.v1011.linuxia64 |
| IBM Cognos BI for Solaris SPARC (32-Bit)                  | com.ibm.ws.cognos.v1011.solaris32 |
| IBM Cognos BI for Solaris SPARC (64-Bit)                  | com.ibm.ws.cognos.v1011.solaris64 |
| IBM Cognos BI for Linux on System z                       | com.ibm.ws.cognos.v1011.zlinux64  |

- b. Ersetzen Sie *installationsverzeichnis* durch die Position, an der Sie das Produkt installiert haben.
- c. Ersetzen Sie *protokollposition* durch die Position und den Dateinamen für die Protokollierung der Informationen.

Installation Manager deinstalliert diese Produktliste und schreibt eine Protokolldatei in das von Ihnen angegebene Verzeichnis.

Im folgenden Beispiel werden IBM Business Monitor, WebSphere Application Server ND und DB2 Express unter Windows deinstalliert.

```
C:\Programme\IBM\Installation Manager\eclipse\tools>imcl uninstall com.ibm.websphere.MON.V80 com.i
```

## Präsentationsmodell entfernen

IBM Business Monitor enthält ein Präsentationsmodell für die Bearbeitung von Hypothekendarlehen ('Mortgage Lending'). Dieses Modell demonstriert einen Teil der Funktionalität von IBM Business Monitor. Sie können dieses Modell über die Konsole 'Erste Schritte' installieren.

Führen Sie folgende Schritte aus, um das Präsentationsmodell zu entfernen:

1. Löschen Sie das Dashboard 'Better Lender' über Business Space Manager.
2. Verwenden Sie die Administrationskonsole von WebSphere Application Server, um die Alertvorlagen zu entfernen.
3. Bei aktivierter Sicherheit müssen Sie die Benutzerrolle in der Administrationskonsole von WebSphere Application Server entfernen.
4. Löschen Sie das Modell mit der Administrationskonsole von WebSphere Application Server.



Gedruckt in Deutschland