

IBM SPSS Collaboration and
Deployment Services 4.2
Administratorhandbuch



Note: Before using this information and the product it supports, read the general information under Notices auf S. 145.

This document contains proprietary information of SPSS Inc, an IBM Company. It is provided under a license agreement and is protected by copyright law. The information contained in this publication does not include any product warranties, and any statements provided in this manual should not be interpreted as such.

When you send information to IBM or SPSS, you grant IBM and SPSS a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright SPSS Inc. 2004, 2010..**

Vorwort

IBM® SPSS® Collaboration and Deployment Services gestattet die weit verbreitete Verwendung und Bereitstellung von Vorhersageanalysen und bietet eine zentrale, sichere und prüffähige Speicherung von Analyseeinrichtungen, erweiterte Funktionen für Verwaltung und Steuerung von Analyseprozessen zur Vorhersage sowie ausgereifte Mechanismen zur Bereitstellung der Ergebnisse der analytischen Verarbeitung für die Endbenutzer.

Das vorliegende Handbuch dokumentiert die Verwaltungsaspekte des Einsatzes von IBM SPSS Collaboration and Deployment Services. Die Informationen sind für Aufgaben wie Einrichten eines Content-Repository-Servers, Verwalten von Benutzern, Konfigurieren von Kommunikationsprotokollen, Installieren von Updates, Auditing des Repository usw. vorgesehen. Die Software- und Hardwareanforderungen für IBM SPSS Collaboration and Deployment Services und die Systeminstallation und Konfiguration sind im *IBM SPSS Collaboration and Deployment Services 4.2-Installations- und Konfigurationshandbuch* beschrieben. Die Aufgaben, die mit der alltäglichen Nutzung der analytischen Einrichtungen von IBM SPSS Collaboration and Deployment Services verbunden sind, werden im *IBM® SPSS® Collaboration and Deployment Services Deployment Manager 4.2-Benutzerhandbuch* beschrieben.

Technischer Support

Registrierte Kunden von SPSS Inc. können den SPSS Inc. Technischen Support in Anspruch nehmen. Kunden können sich an den technischen Support wenden, wenn sie Hilfe bei der Arbeit mit SPSS Inc.-Produkten oder bei der Installation in einer der unterstützten Hardware-Umgebungen benötigen. Informationen zum Technischen Support finden Sie auf der SPSS Inc.-Website unter <http://www.spss.com> oder wenden Sie sich an Ihr regionales Büro, das Sie auf der SPSS Inc.-Website unter <http://www.spss.com/worldwide> finden. Beachten Sie, dass Sie nach Ihrem Namen, dem Namen Ihrer Organisation und Ihrer Seriennummer gefragt werden.

Kundenmeinungen

Ihre Meinung ist uns wichtig. Teilen Sie uns bitte Ihre Erfahrungen mit SPSS Inc.-Produkten mit. Senden Sie uns eine E-Mail an suggest@us.ibm.com oder schreiben Sie an: SPSS Inc., Attn: Director of Product Planning, 233 South Wacker Drive, 11th Floor, Chicago, IL 60606-6412.

1	Übersicht	1
	IBM SPSS Collaboration and Deployment Services	1
	Zusammenarbeit	1
	Bereitstellung	2
	Systemarchitektur	3
	IBM SPSS Collaboration and Deployment Services Repository	4
	IBM SPSS Collaboration and Deployment Services Deployment Manager	4
	IBM SPSS Collaboration and Deployment Services Deployment Portal	4
	Browserbasiertes IBM SPSS Collaboration and Deployment Services Deployment Manager	5
	IBM SPSS Collaboration and Deployment Services Enterprise View	5
	Ausführungsserver	6
	BIRT Report Designer for IBM SPSS	6
	Produkte mit Collaboration	7
2	Neuerungen in dieser Version	8
	Neuerungen in Version 4.2	8
3	Erste Schritte	9
	Starten von IBM SPSS Collaboration and Deployment Services Repository	9
	Stoppen von IBM SPSS Collaboration and Deployment Services Repository	12
	Verwendung des browserbasierten IBM SPSS Collaboration and Deployment Services Deployment Manager	13
	Ändern von Passwörtern	14
	Navigation durch das browserbasierte IBM SPSS Collaboration and Deployment Services Deployment Manager	15
	Zugriff auf Systeminformationen	16
	Verwendung von IBM SPSS Collaboration and Deployment Services Deployment Manager	17
	Verwaltete Server	17
	Hinzufügen von neuen verwalteten Servern	18
	Anzeigen von Eigenschaften des verwalteten Servers	21
	Verbinden mit verwalteten Servern	22

Trennen der Verbindung zu verwalteten Servern	22
Löschen von verwalteten Servern	23
Namenskonventionen	23
4 Benutzer und Gruppen	25
Einrichten von IBM SPSS Collaboration and Deployment Services-Benutzern	26
Verwalten von Benutzern und Gruppen in IBM SPSS Collaboration and Deployment Services Deployment Manager	26
Erstellen eines Benutzers	29
Bearbeiten eines Benutzers	31
Löschen eines Benutzers	33
Erstellen einer Gruppe	33
Bearbeiten einer Gruppe	34
Löschen einer Gruppe	36
Importieren von Benutzern und Gruppen	36
Erstellen einer erweiterten Gruppe	37
Erstellen eines erlaubten Benutzers	38
5 Rollen	40
Überblick über Rollen	40
Aktionen	40
Administrator-Rolle	42
Rollendefinitionen verwalten	42
Erstellen einer neuen Rolle	43
Bearbeiten einer Rolle	45
Bearbeiten von Benutzern und Gruppen, die einer Rolle zugewiesen sind	45
Entfernen einer Rolle	47
6 Sicherheits-Provider	48
Sicherheits-Provider in IBM SPSS Collaboration and Deployment Services Deployment Manager	49
Konfigurieren von Sicherheits-Providern	49
Sicherheits-Provider im browserbasierten IBM SPSS Collaboration and Deployment Services Deployment Manager	56
Konfigurieren von Sicherheits-Providern	56

7 Einzelanmeldung 60

Konfigurieren von Einzelanmeldungen	60
---	----

8 Repository-Konfiguration 62

Administrator	63
BIRT Report Designer für IBM SPSS	63
Cache-Provider	64
Benutzerdefinierte Dialogfelder	65
Datenservice	66
Deployment Manager	67
Deployment Portal	67
Deployment Portal-Scoring	68
Enterprise-Ansicht	68
Hilfe	70
Benachrichtigung	70
Pager	76
Prozessmanagement	77
Reporting	79
Repository	79
Scoring-Service	82
Suchen	83
Sicherheit	84
Setup	85
IBM ShowCase	86
CMOR	87

9 MIME-Typen 89

Hinzufügen von MIME-Typzuordnungen	90
Bearbeiten von MIME-Typzuordnungen	91
Löschen von MIME-Typzuordnungen	92

10 Neuindizierung des Repository 93

11 Benachrichtigungen 95

Struktur von Benachrichtigungsmeldungsvorlagen	95
Meldungseigenschaften	96
Meldungsinhalt	98
Meldungsformat	100
Bearbeiten von Benachrichtigungsvorlagen	102
Jobstatus	103
Optimieren der Leistung des Benachrichtigungsdienstes	105
Konfiguration des Benachrichtigungsdienstes	105
Allgemeine Empfehlungen	107
Fehlersuche im Benachrichtigungsdienst	109
Fehlerbehebung bei fehlgeschlagener Benachrichtigungszustellung	110

12 JMS-Setup 111

JMS-Thema-Konfiguration	111
IBM SPSS Collaboration and Deployment Services-Setup	112
JMS-Client-Beispielprogramm	112
Ausführen des Beispielprogramms	114
Beispiel für meldungsbasierte Verarbeitung	114

13 Auditing des Repository 116

Datenbank-Audit-Möglichkeiten	116
Audit-Ereignisse	117
Ereignistabellen	118
Audit-Ansichten	120
Audit (SPSSPLAT_V_AUDIT)	121
Benutzerdefinierte Eigenschaft (SPSSPLAT_V_CUSTOMPROPERTY)	122
Dateiversion (SPSSPLAT_V_FILEVERSION)	122
Jobverlauf (SPSSPLAT_V_JOBHISTORY)	123
Jobschritt (SPSSPLAT_V_JOBSTEP)	124
Zeitplan (SPSSPLAT_V_SCHEDULE)	124

Stream-Attributwert (SPSSPLAT_V_STREAMATTRVALUE)	125
Stream-Knoten (SPSSPLAT_V_STREAMNODE)	126
Scoring-Serviceprotokollierung	127
Protokollierungstabelle für Anforderungen	127
Datenbankansichten	128
Beispiele für Audit-Abfragen	131

Anhänge

A Fehlerbehebung 133

Fehlerbehebung beim Repository	133
Solaris	136
HP-UX	136
Oracle-Datenbank	137
JBoss	137
WebLogic	138
WebSphere	139

B Nativestore-Schema-Referenz 141

nativestore-Element	141
user-Element	141
obsolete-Element	143

C Notices 145

Index 147

Übersicht

IBM SPSS Collaboration and Deployment Services

IBM® SPSS® Collaboration and Deployment Services ist eine Anwendung auf Unternehmensebene, die eine breite Verwendung und Implementierung von Vorhersageanalysen ermöglicht. IBM SPSS Collaboration and Deployment Services ermöglicht eine zentrale, sichere und Audit-fähige Speicherung von Analyseeinrichtungen, erweiterte Funktionen für die Verwaltung und Steuerung von Analyseprozessen zur Vorhersage sowie ausgereifte Mechanismen zur Bereitstellung der Ergebnisse der analytischen Verarbeitung für die Endbenutzer. Die Vorteile von IBM SPSS Collaboration and Deployment Services:

- Schutz des Werts von Analyseeinrichtungen
- Sichere Einhaltung von Bestimmungen
- Höhere Produktivität der Analytiker
- Minimierte IT-Kosten für die Analyseverwaltung

IBM SPSS Collaboration and Deployment Services ermöglicht Ihnen die sichere Verwaltung verschiedener Analyseeinrichtungen und fördert die Zusammenarbeit zwischen den Entwicklern und den Benutzern. Darüber hinaus stellen die Bereitstellungseinrichtungen sicher, dass die richtigen Personen die benötigten Informationen erhalten, um rechtzeitig die korrekten Aktionen auszuführen.

Zusammenarbeit

Zusammenarbeit bezieht sich auf die Fähigkeit, Analyseeinrichtungen effizient gemeinsam zu benutzen und wiederholt zu benutzen. Sie ist der Schlüssel zur Entwicklung und Implementierung von Analysen in einem Unternehmen. Analytiker brauchen einen Ort, an den sie Dateien platzieren können, die anderen Analytikern oder Unternehmensanwendern zur Verfügung stehen sollen. An diesem Ort muss eine Versionskontrolle für die Dateien implementiert werden, um die Weiterentwicklung der Analyse zu verwalten. Sicherheit ist erforderlich, um Zugriff auf die Dateien und Änderung der Dateien zu steuern. Schließlich wird noch ein Sicherheits- und Wiederherstellungsmechanismus benötigt, um das Unternehmen vor dem Verlust dieser bedeutenden Daten zu schützen.

Zur Erfüllung dieser Anforderungen bietet IBM® SPSS® Collaboration and Deployment Services ein Repository zum Speichern dieser Informationen in einer Ordnerhierarchie ähnlich den meisten Dateisystemen zur Organisation. Dateien, die im IBM® SPSS® Collaboration and Deployment Services Repository gespeichert sind, stehen im gesamten Unternehmen zur

Verfügung, vorausgesetzt die Benutzer verfügen über die entsprechenden Zugriffsrechte. Zum Auffinden der gewünschten Informationen bietet das Repository eine Suchfunktion.

Analytiker können die Dateien im Repository mithilfe von Clientanwendungen bearbeiten, welche die Serviceschnittstelle von IBM SPSS Collaboration and Deployment Services nutzen. Produkte wie IBM® SPSS® Statistics und IBM® SPSS® Modeler ermöglichen direkte Interaktion mit Dateien im Repository. Ein Analytiker kann eine Version einer in Entwicklung befindlichen Datei speichern, diese Version zu einem späteren Zeitpunkt abrufen und mit deren Bearbeitung fortfahren, bis sie abgeschlossen ist und in einen Produktionsprozess verlagert werden kann. Diese Dateien können benutzerdefinierte Oberflächen enthalten, die Analyseprozesse ausführen und Unternehmensanwendern erlauben, die Vorteile aus der Arbeit eines Analytikers zu nutzen.

Der Einsatz des Repository schützt das Unternehmen, indem es einen zentralen Speicherort für Analyseeinrichtungen bietet, der sich bequem sichern und wiederherstellen lässt. Zudem steuern Berechtigungen auf Benutzer-, Datei- und Versionsebene den Zugriff auf die individuellen Bereiche. Versionssteuerung und Objektversionsbezeichnungen stellen sicher, dass die korrekten Versionen der Daten in Produktionsprozessen verwendet werden. Und die Protokollierungsfunktionen bieten die Möglichkeit, Datei- und Systemänderungen zu verfolgen.

Bereitstellung

Damit alle Vorteile der Vorhersageanalyse nutzbar sind, müssen die Analyseeinrichtungen Input für Geschäftsentscheidungen liefern. Die Bereitstellung überbrückt die Lücke zwischen Analyse und Aktion, indem sie die Ergebnisse nach einem Zeitplan oder in Echtzeit an Personen und Prozesse übergibt.

In IBM® SPSS® Collaboration and Deployment Services können individuelle Dateien, die im Repository gespeichert sind, in die Verarbeitung von **Jobs** eingeschlossen werden, die eine Ausführungssequenz für die Dateien definieren. Die Ausführungsergebnisse können im Repository oder auf einem Dateisystem gespeichert oder an angegebene Empfänger übergeben werden. Auf die im Repository gespeicherten Ergebnisse kann jeder Benutzer mit den entsprechenden Berechtigungen über die IBM® SPSS® Collaboration and Deployment Services Deployment Portal-Benutzeroberfläche zugreifen. Die Jobs können nach einem definierten Zeitplan oder als Reaktion auf Systemereignisse ausgelöst werden.

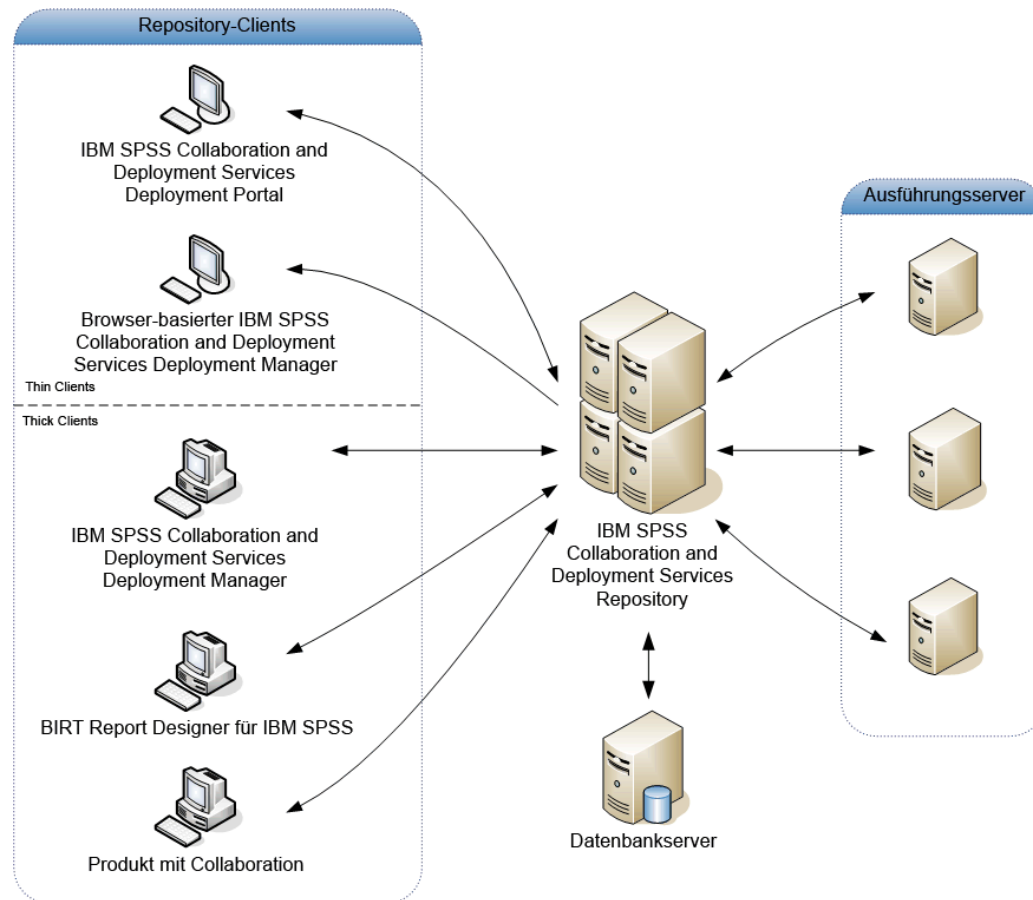
Zusätzlich gestattet der Scoring-Service von IBM SPSS Collaboration and Deployment Services, dass Analyseergebnisse von bereitgestellten Modellen bei der Interaktion mit einem Kunden in Echtzeit geliefert werden. Ein für Scoring konfiguriertes Analysemodell kann Daten, die in einer aktuellen Kundeninteraktion erfasst werden, mit historischen Daten kombinieren und so einen Score erzeugen, der den Verlauf der Interaktion bestimmt. Den Service selbst kann eine beliebige Clientanwendung nutzen und ermöglicht es, spezielle Schnittstellen zur Definition des Prozesses zu erstellen.

Die Bereitstellungsfunktionen von IBM SPSS Collaboration and Deployment Services sind so konzipiert, dass sie sich einfach in Ihre Unternehmensinfrastruktur integrieren lassen. Durch Einzelanmeldungen reduzieren sich manuelle Eingaben von Anmeldedaten in verschiedenen Stadien des Prozesses. Darüber hinaus kann das System so konfiguriert werden, dass es mit dem Federal Information Processing Standard Publication 140-2 konform ist.

Systemarchitektur

Generell besteht IBM® SPSS® Collaboration and Deployment Services aus einem einzigen, zentralen IBM® SPSS® Collaboration and Deployment Services Repository, das eine Vielzahl von Clients mithilfe von Ausführungsservern zur Verarbeitung von Analyseeinrichtungen bedient.

Abbildung 1-1
IBM SPSS Collaboration and Deployment Services-Architektur



IBM SPSS Collaboration and Deployment Services besteht aus folgenden Komponenten:

- IBM SPSS Collaboration and Deployment Services Repository für analytische Artefakte
- Produkt mit Collaboration
- IBM® SPSS® Collaboration and Deployment Services Deployment Manager
- IBM® SPSS® Collaboration and Deployment Services Deployment Portal
- Browserbasiertes IBM® SPSS® Collaboration and Deployment Services Deployment Manager
- IBM® SPSS® Collaboration and Deployment Services Enterprise View
- BIRT Report Designer for IBM® SPSS®

IBM SPSS Collaboration and Deployment Services Repository

Das Repository ist ein zentraler Ort, an dem Analyseeinrichtungen, wie Modelle und Daten, gespeichert werden können. Das Repository umfasst Funktionen für:

- Sicherheit
- Versionskontroller
- Suchen
- Auditing

Das Repository erfordert die Installation einer relationalen Datenbank wie Oracle, IBM DB2 UDB oder Microsoft SQL Server.

Konfigurationsoptionen für das Repository werden über das IBM® SPSS® Collaboration and Deployment Services Deployment Manager oder das browserbasierte IBM® SPSS® Collaboration and Deployment Services Deployment Manager definiert. Der Inhalt des Repository wird über das Deployment Manager verwaltet und IBM® SPSS® Collaboration and Deployment Services Deployment Portal wird verwendet, um darauf zuzugreifen.

IBM SPSS Collaboration and Deployment Services Deployment Manager

IBM® SPSS® Collaboration and Deployment Services Deployment Manager ist eine Client-Anwendung, die es Benutzern ermöglicht, analytische Aufgaben, wie die Aktualisierung von Modellen oder Scores, mithilfe des Repository zu planen, zu automatisieren und auszuführen. Der Client ermöglicht einem Benutzer Folgendes:

- Anzeigen vorhandener Dateien innerhalb des Systems, darunter -Berichte, SAS-Syntaxdateien, und Datendateien
- Importieren von Dateien in das Repository
- Planung wiederholt auszuführender Jobs mithilfe eines bestimmten Zeitmusters, z. B. vierteljährlich oder stündlich
- Änderung vorhandener Job-Eigenschaften in einer benutzerfreundlichen Bedienoberfläche
- Bestimmen des Status eines Jobs
- Definieren von E-Mail-Benachrichtigungen über den Job-Status

Außerdem ermöglicht die Clientanwendung den Benutzern, administrative Aufgaben für IBM® SPSS® Collaboration and Deployment Services auszuführen, darunter:

- Benutzerverwaltung
- Konfiguration von Sicherheits-Providern
- Zuordnung von Rollen und Aktionen

IBM SPSS Collaboration and Deployment Services Deployment Portal

IBM® SPSS® Collaboration and Deployment Services Deployment Portal ist eine Thin-Client-Benutzeroberfläche für den Zugriff auf das Repository. Im Gegensatz zum browserbasierten IBM® SPSS® Collaboration and Deployment Services Deployment Manager,

das für Administratoren gedacht ist, ist Deployment Portal ein Webportal, das einer Vielzahl von Benutzern zur Verfügung steht. Das Webportal beinhaltet die folgenden Funktionen:

- Durchsuchen des Repository-Inhalts nach Ordner
- Öffnen von veröffentlichtem Content
- Ausführen von Jobs und Berichten
- Generieren von Scores anhand von im Repository gespeicherten Modellen
- Durchsuchen des Repository-Inhalts
- Anzeigen von Content-Eigenschaften
- Zugriff auf individuelle Benutzereinstellungen wie E-Mail-Adresse und Passwort, auf allgemeine Optionen, Abonnements und Optionen für Ausgabedateiformate

Browserbasiertes IBM SPSS Collaboration and Deployment Services Deployment Manager

Das browserbasierte IBM® SPSS® Collaboration and Deployment Services Deployment Manager ist eine Thin-Client-Benutzeroberfläche für die Ausführung von Einrichtungs- und Systemmanagementaufgaben wie:

- Konfigurieren des Systems
- Konfigurieren von Sicherheits-Providern
- Verwalten von MIME-Typen

Nicht administrative Benutzer können all diese Aufgaben ausführen, wenn die entsprechenden Aktionen ihren Anmeldeinformationen zugeordnet sind. Die Aktionen werden von einem Administrator zugewiesen.

IBM SPSS Collaboration and Deployment Services Enterprise View

Die IBM® SPSS® Collaboration and Deployment Services Enterprise View bietet einen zentralen, konsistenten Überblick über Unternehmensdaten. Damit können die Benutzer eine allgemeine Ansicht von Warehouse- und Transaktionsdaten definieren und aufrechterhalten, die für die Durchführung von Analysen, Optimierung, Bereitstellung und Berichterstellung benötigt werden. Die zugrunde liegenden Daten können aus einer Vielzahl von Quellen stammen, z. B. aus einem Data Warehouse, einem Operational Data Store oder einer Online-Transaktionsdatenbank. Die Enterprise-Ansicht gewährleistet eine konsistente Verwendung von Unternehmensdaten und blendet die komplexen Merkmale gespeicherter Datenstrukturen gegenüber dem Endbenutzer aus. Die Enterprise-Ansicht ist das "Daten-Rückgrat" für ein Unternehmen, das auf Vorhersageanalysen setzt.

Data-Discovery erfordert einen erheblichen Ressourcenaufwand seitens der Organisationen, die Vorhersageanalysen einsetzen. Das Verfahren ist arbeitsintensiv — u. U. müssen Vertreter von Abteilungen aus dem gesamten Unternehmen einbezogen werden und es erfordert häufig die Auflösung von Unterschieden in der Datenstruktur oder -semantik über die Organisationsgrenzen hinweg. Die Enterprise-Ansicht bietet eine Methode für die Aufzeichnung der Ergebnisse

des Data-Discovery-Verfahrens, für die Versionsverwaltung und die Sicherung des daraus resultierenden Schemas sowie für die Nachverfolgung von Änderungen im Laufe der Zeit.

Die Enterprise-Ansicht enthält die IBM® SPSS® Collaboration and Deployment Services Enterprise View Driver-Komponente, die anderen Anwendungen den Zugriff auf Enterprise-Ansicht-Objekte ermöglicht, die im Repository gespeichert sind. Der Treiber funktioniert ähnlich wie ODBC-Treiber, mit der Ausnahme, dass er nicht direkt eine physische Datenquelle abfragt, sondern vielmehr Enterprise-Ansicht Daten-Provider-Definitionen und Application-Ansichtn referenziert. Beachten Sie, dass die Enterprise-Ansicht zwar als Teil von IBM® SPSS® Collaboration and Deployment Services Deployment Manager installiert wird, der Enterprise-Ansicht-Treiber jedoch separat installiert werden muss. Weitere Informationen finden Sie in den Installationsanweisungen.

Ausführungsserver

Ausführungsserver ermöglichen die Ausführung von Ressourcen, die im Repository gespeichert sind. Wenn eine Ressource zur Ausführung in einen Job eingeschlossen ist, umfasst die Jobschritt-Definition die Angabe des Ausführungsservers, der den Schritt verarbeitet. Der Typ des Ausführungsservers hängt von der Ressource ab.

Durch IBM® SPSS® Collaboration and Deployment Services unterstützte Ausführungsserver sind:

- **SAS.** Der SAS-Ausführungsserver ist die ausführbare SAS-Datei *sas.exe*, die Teil der Basis-SAS®-Software ist. Verwenden Sie diesen Ausführungsserver, um SAS-Syntaxdateien zu verarbeiten.
- **Fernverarbeitung.** Ein Ausführungsserver für Fernverarbeitungen ermöglicht den Start und die Überwachung von Prozessen auf Remote-Servern. Nach Abschluss des Prozesses gibt er eine Erfolgs- bzw. Fehlschlagsmeldung zurück. Auf allen Rechnern, die als Fernverarbeitungsserver fungieren, muss die zur Kommunikation mit dem Repository benötigte Infrastruktur installiert sein.

Ausführungsserver, die andere spezifische Typen von Ressourcen verarbeiten, lassen sich dem System durch Installieren der entsprechenden Adapter hinzufügen. Weitere Informationen finden Sie in der Dokumentation zu diesen Ressourcentypen.

Ordnen Sie während einer Joberstellung jedem im Job enthaltenen Schritt einen Ausführungsserver zu. Bei der Ausführung des Jobs verwendet das Repository die angegebenen Ausführungsserver für die Ausführung der entsprechenden Analysen.

BIRT Report Designer for IBM SPSS

Die Berichtfunktionalität von IBM® SPSS® Collaboration and Deployment Services wird von BIRT (Business Intelligence and Reporting Tools) bereitgestellt. Dabei handelt es sich um ein Open-Source-Paket, das von der Eclipse Foundation im Rahmen der Eclipse Public License vertrieben wird. BIRT bietet zentrale Berichtfunktionen, wie z. B. Berichtgestaltung, Datenzugriff und Skriptnutzung. Weitere Informationen zu BIRT finden Sie auf der [Seite zum BIRT-Projekt \(http://www.eclipse.org/birt\)](http://www.eclipse.org/birt).

Die Installation von IBM SPSS Collaboration and Deployment Services beinhaltet die BIRT Bericht-Engine-Serverkomponenten, die für die Ausführung von BIRT Berichtsyntaxdateien im Rahmen der Bericht-Job-Schritte in IBM SPSS Collaboration and Deployment Services erforderlich sind. BIRT Report Designer for IBM® SPSS® ist eine Einzelanwendung, die zusammen mit IBM SPSS Collaboration and Deployment Services verwendet werden kann. Die Anwendung verfügt über eine umfassende Benutzeroberfläche mit erweiterten Funktionen zur Erstellung von Berichten und muss separat installiert werden.

Wenn ein BIRT Report Designer for IBM SPSS-Bericht eine JDBC-basierte Datenbankverbindung erfordert, muss ein entsprechender JDBC-Treiber mit dem IBM® SPSS® Collaboration and Deployment Services Repository installiert werden. Anwendungsserverspezifische Informationen zum Speicherort der JDBC-Treiber finden Sie im entsprechenden Abschnitt der Repository-Installationsanweisungen.

Um BIRT Report Designer for IBM SPSS zu starten, führen Sie die Datei *BIRT.exe* im Installationsverzeichnis aus. Informationen zur Verwendung von BIRT Report Designer for IBM SPSS finden Sie in der Dokumentation, die zusammen mit der Anwendung installiert wurde.

Produkte mit Collaboration

Ein Produkt mit Collaboration erlaubt die Interaktion mit dem IBM® SPSS® Collaboration and Deployment Services Repository von der nativen -Oberfläche aus. Dateien können direkt im Kollaborationsprodukt gespeichert und von dort abgerufen werden.

Zusätzlich können einige Dateien, die im Repository gespeichert sind, als Schritte in Jobs ausgeführt werden. Ein Job kann eine beliebige Anzahl von Schritten enthalten, wobei jeder Schritt einer separaten Datei entspricht. Beziehungen, die zwischen den Schritten definiert sind, bestimmen den Verarbeitungsablauf. Der Job kann zur Ausführung zu einem bestimmten Zeitpunkt nach einem wiederkehrenden Muster geplant werden oder als Reaktion auf ein definiertes Ereignis ausgeführt werden. Darüber hinaus können Benachrichtigungen an angegebene Empfänger gesendet werden, um über individuelle Schritte oder den Gesamtausführungsstatus eines Jobs zu berichten.

Zusammenarbeit zwischen IBM® SPSS® Collaboration and Deployment Services und anderen Produkten wird durch die Verwendung von Adaptern ermöglicht. Diese Adapter werden in der IBM SPSS Collaboration and Deployment Services-Umgebung installiert, um die produktspezifischen Funktionen hinzuzufügen. Weitere Informationen finden Sie in der Dokumentation zum Kollaborationsprodukt.

Neuerungen in dieser Version

Neuerungen in Version 4.2

Folgende Erweiterungen wurden der Anwendung hinzugefügt:

Mit dieser Version wird PASW Collaboration and Deployment Services in IBM® SPSS® Collaboration and Deployment Services umbenannt. In der folgenden Tabelle sind die neuen Namen für Funktionen aufgeführt, die in den vorangegangenen Versionen eingeführt wurden.

Alter Name	Neuer Name	Allgemeine Verwendung
PASW Collaboration and Deployment Services	IBM SPSS Collaboration and Deployment Services	IBM SPSS Collaboration and Deployment Services
Deployment Manager	IBM® SPSS® Collaboration and Deployment Services Deployment Manager	Deployment Manager
Deployment Portal	IBM® SPSS® Collaboration and Deployment Services Deployment Portal	Deployment Portal
Browserbasierter Deployment Manager	Browserbasiertes IBM® SPSS® Collaboration and Deployment Services Deployment Manager	Browserbasiertes Deployment Manager
PASW BIRT Report Designer	BIRT Report Designer for IBM® SPSS®	BIRT Report Designer for IBM SPSS
PASW Tag-Bibliothek	IBM® SPSS® Collaboration and Deployment Services Tag Library	IBM SPSS Collaboration and Deployment Services Tag Library
Repository	IBM® SPSS® Collaboration and Deployment Services Repository	IBM SPSS Collaboration and Deployment Services Repository
Enterprise-Ansicht	IBM® SPSS® Collaboration and Deployment Services Enterprise View	IBM SPSS Collaboration and Deployment Services Enterprise View

RSS-Benachrichtigungen

IBM SPSS Collaboration and Deployment Services gestattet Benutzern nun das Abonnieren von RSS-(Real Simple Syndication-)Benachrichtigungsfeeds, um über Änderungen an Repository-Inhalten und den Verarbeitungsstatus informiert zu werden. So können Benachrichtigungen in benutzerdefinierte, browserbasierte Oberflächen und Dashboards integriert werden. Zudem können RSS-Feeds gefiltert werden, um nur bestimmte Benachrichtigungstypen anzuzeigen. So kann ein Benutzer, der sich nur für Meldungen über den Erfolg oder Misserfolg eines Jobs interessiert, inhaltsbezogene Benachrichtigungen herausfiltern.

Erste Schritte

Nach der erfolgreichen Installation des IBM® SPSS® Collaboration and Deployment Services Repository können die folgenden Aktionen ausgeführt werden:

- Starten des Servers als Konsolenanwendung oder -service
- Stoppen des Servers als Konsolenanwendung oder -service
- Anmeldung und Abmeldung beim System
- Ändern von Passwörtern und Navigieren in der Oberfläche
- Hinzufügen oder Ändern von IBM® SPSS® Modeler-Unterstützung

Starten von IBM SPSS Collaboration and Deployment Services Repository

Das Repository kann an einer Konsole oder im Hintergrund ausgeführt werden. Die Ausführung an einer Konsole ermöglicht die Anzeige von Verarbeitungsmeldungen und kann nützlich für die Diagnose von unvorhergesehenem Verhalten sein. Jedoch wird das Repository in der Regel im Hintergrund ausgeführt und verarbeitet Anforderungen von Clients wie z. B. IBM® SPSS® Modeler oder IBM® SPSS® Collaboration and Deployment Services Deployment Manager.

Anmerkung: Die gleichzeitige Ausführung anderer Anwendungen kann die Systemleistung und die Startgeschwindigkeit verringern.

Auf der Windows-Plattform entspricht die Ausführung an einer Konsole der Ausführung in einem Befehlsfenster. Die Ausführung im Hintergrund entspricht der Ausführung als Windows-Dienst. Im Unterschied dazu entspricht an einer UNIX-Plattform die Ausführung an einer Konsole der Ausführung in einer Shell, und die Ausführung im Hintergrund entspricht der Ausführung als Daemon.

Anmerkung: Zur Vermeidung von Berechtigungskonflikten auf UNIX-Systemen muss das Repository immer mit denselben Anmeldeinformationen gestartet werden, vorzugsweise als *root*.

Das Repository kann mithilfe der Skripts gestartet werden, die mit der Installation oder nativen Anwendungsserver-Administrationstools geliefert werden, z. B. mit WebLogic Server Administration Console. Weitere Informationen finden Sie in der Herstellerdokumentation zum Anwendungsserver.

Starten eines Service unter Windows

Für eine Installation mithilfe von JBoss starten Sie das Repository folgendermaßen als Dienst unter Windows:

1. Öffnen Sie die Windows-Dienste-Konsole.
2. Wählen Sie IBM SPSS Collaboration and Deployment Services Server aus der Liste verfügbarer Dienste.
3. Legen Sie als "Starttyp" Automatisch fest. Das ermöglicht den Repository-Start beim Booten des Systems.
4. Falls derzeit nicht aktiv, klicken Sie auf Starten.

Anmerkung: Es kann mehrere Minuten dauern, bis der Server und seine Komponenten aktiv sind.

5. Klicken Sie auf OK, um die Änderungen zu übernehmen und das Dialogfeld zu schließen.

Für eine Installation mithilfe von WebLogic muss der *SPSSDomain*-Server als Windows-Service eingerichtet werden. Weitere Informationen finden Sie in der [WebLogic-Dokumentation](http://e-docs.bea.com/wls/docs81/adminguide/winservice.html) (<http://e-docs.bea.com/wls/docs81/adminguide/winservice.html>).

Konfigurationsinformationen zum automatischen Start von WebSphere finden Sie in der [WebSphere-Dokumentation](http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp) (<http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp>).

Starten eines Daemon unter UNIX

Informationen zum Starten des Repository-Daemon auf einem von JBoss abweichenden Anwendungsserver erhalten Sie in der Dokumentation des Serverherstellers.

So starten Sie das Repository als Daemon unter UNIX für eine Installation mit JBoss:

1. Navigieren Sie von einer Befehlszeile aus in das Verzeichnis *bin* der JBoss-Installation.
2. Geben Sie Folgendes ein:

```
./mm.sh start
```

Anmerkung: Es kann mehrere Minuten dauern, bis der Server und seine Komponenten aktiv sind.

3. Um zu verifizieren, dass der Server aktiv ist, schreiben Sie `ps -e | grep wrapper`. Wenn er aktiv ist, wird der Prozess in der Liste angezeigt.

Starten unter IBM i

Die WebSphere-Instanz, die IBM® SPSS® Collaboration and Deployment Services auf IBM i ausführt, wird durch die Ausführung von ähnlichen Befehlen wie den folgenden in der QShell-Umgebung gestartet:

```
cd /QIBM/UserData/WebSphere/AppServer/V61/Base/profiles/<profilname>/bin  
./startServer <profilname>
```

So konfigurieren Sie Anwendungsserver für automatischen Start, wenn QWAS61 (WebSphere-Application-Server-Subsystem) startet:

1. Erteilen Sie Ihrem Benutzerprofil die Berechtigung für die Jobbeschreibung QWAS61/QWASJOB0 und die Subsystembeschreibung QWAS61/QWAS61.
2. Erstellen Sie für jedes Profil ein Duplikat der Jobbeschreibung, die von WebSphere-Application-Server-Profilen verwendet wird. Verwenden Sie den folgenden Befehl in der Befehlszeile:

```
CRTDUPOBJ OBJ(QWASJOB0) FROMLIB(QWAS61) OBJTYPE(*JOB0) TOLIB(mywasjob0) NEWOBJ(myserver)
```

3. Verwenden Sie den Befehl CHGJOB0, um die neu erstellte Jobbeschreibung so zu ändern, dass das Feld für die Anforderungsdaten oder den Anforderungsbefehl (RQSDTA) den neuen Server startet. Um beispielsweise den Anwendungsserver (server1) des Standardprofils beim Start des Subsystems zu starten, legen Sie das Feld RQSDTA wie folgt fest:

```
'QSYS/CALL PGM(product_library/QWASSTRSVR) PARM(-profilePath user_data_root/profiles/default-serverserver1)'
```

4. Fügen Sie einen autostart-Jobeintrag zum Subsystem QWAS61/QWAS61 hinzu. Geben Sie den folgenden Befehl in die CL-Befehlszeile ein:

```
ADDAJE SBS0(QWAS61/QWAS61) JOB(myserver) JOB0(mywasjob0/myserver)
```

Optional: Konfigurieren Sie das System so, dass das Subsystem QWAS61 während des Systemstarts startet. Um automatischen Start zu aktivieren, fügen Sie dem Systemstartprogramm die folgende Zeile hinzu: STRSBS QWAS61/QWAS61.

Anmerkung: Das Systemstartprogramm wird durch den Systemwert QSTRUPPGM definiert. TCP/IP muss aktiv sein, bevor das WebSphere-Application-Server-Subsystem starten kann. Stellen Sie sicher, dass der Befehl STRTCP vor dem Befehl STRSBS QWAS61/QWAS61 in Ihrem Startprogramm oder Ihrem Autostart-Job ausgeführt wird.

Anmerkung: Diese Befehle können beliebigen rc-Skripts zum Starten oder Beenden hinzugefügt werden.

Starten einer Konsolenanwendung unter Windows

So starten Sie das Repository als Konsolenanwendung unter Windows:

1. Führen Sie im Repository-Installationspfad die Datei *startserver.bat* aus. Die Stapeldatei öffnet ein Befehlszeilenfenster und startet den Server.

Anmerkung: Es kann mehrere Minuten dauern, bis der Server und seine Komponenten vollständig geladen sind.

2. Prüfen Sie, ob der Server aktiv ist, indem Sie einen Browser öffnen. Der Anmeldebildschirm wird geöffnet, wenn die IP-Adresse und die Portnummer in das Feld URL eingegeben werden.

Starten einer Konsolenanwendung unter UNIX

So starten Sie das Repository als Konsolenanwendung unter UNIX:

1. Navigieren Sie in der Befehlszeile zum Repository-Installationsverzeichnis und führen Sie die Datei *startserver.sh* aus. Das Shellskript wird ausgeführt und der Server gestartet.

Anmerkung: Es kann mehrere Minuten dauern, bis der Server und seine Komponenten vollständig geladen sind.

2. Um zu verifizieren, dass der Server aktiv ist, schreiben Sie `ps -e | grep wrapper`. Wenn er aktiv ist, wird der Prozess in der Liste angezeigt.

Stoppen von IBM SPSS Collaboration and Deployment Services Repository

Das Repository wird über die Befehlszeilenkonsole angehalten oder über das Service-Menü gestoppt.

Stoppen des Service unter Windows

So halten Sie eine aktive Instanz des Repository an:

1. Öffnen Sie die Windows-Dienste-Konsole.
2. Wählen Sie IBM® SPSS® Collaboration and Deployment Services Server aus der Liste verfügbarer Dienste.
3. Klicken Sie auf Stopp, um den Service anzuhalten.

Anmerkung: Es kann mehrere Minuten dauern, bis der Server und seine Komponenten komplett angehalten sind.

Stoppen des Daemon unter UNIX

Informationen zum Stoppen des Repository-Daemon auf einem von JBoss abweichenden Anwendungsserver erhalten Sie in der Dokumentation des Serverherstellers.

So halten Sie eine aktive Instanz des Repository für eine Installation mit JBoss an:

1. Navigieren Sie von einer Befehlszeile aus in das Verzeichnis *bin* der JBoss-Installation.
2. Geben Sie Folgendes ein:

```
./mm.sh stop
```

3. Um zu verifizieren, dass der Server angehalten wurde, schreiben Sie `ps -e | grep wrapper`. Der Prozess darf nicht in der Liste angezeigt sein.

Stoppen unter IBM i

Die WebSphere-Instanz, die IBM SPSS Collaboration and Deployment Services auf IBM i ausführt, wird durch die Ausführung von ähnlichen Befehlen wie den folgenden in der QShell-Umgebung gestoppt:

```
cd /QIBM/UserData/WebSphere/AppServer/V61/Base/profiles/<profilname>/bin
./stopServer <profilname>
```

Stoppen der Konsolenanwendung unter Windows

So halten Sie eine aktive Instanz des Repository an:

1. Öffnen Sie das entsprechende Befehlszeilenfenster und drücken Sie die Tastenkombination Ctrl-C. Dies signalisiert der Befehlszeile, den Prozess zu beenden.
2. Geben Sie Y ein, wenn Sie dazu aufgefordert werden.

Stoppen der Konsolenanwendung unter UNIX

Um eine aktive Instanz des Repository anzuhalten, verwenden Sie die Tastenkombination STRG-C für die Konsole.

Anmerkung: Es kann mehrere Minuten dauern, bis der Server und seine Komponenten komplett angehalten sind.

Verwendung des browserbasierten IBM SPSS Collaboration and Deployment Services Deployment Manager

Die Anmeldungsseite ist Ihr Gateway zum System. So melden Sie sich an:

- Navigieren Sie zur Anmeldungsseite. Der URL lautet normalerweise `http://<host IP address>:<port number>/security/login`. Die Anmeldungsseite wird geöffnet. Beachten Sie, dass die Verwendung von `localhost` anstelle der IP-Adresse für einige Anwendungsserver fehlschlagen kann. Es wird in allen Fällen die Verwendung der IP-Adresse empfohlen.

Abbildung 3-1
Dialogfeld "Anmeldung"

Anmeldung in Deployment Portal

Anmeldename:

Kennwort:

Anmelden

[Kennwort ändern?](#)

Licensed Materials - Property of SPSS Inc., an IBM Company. © Copyright 2004, 2010 SPSS Inc., an IBM Company. IBM and the IBM logo are trademarks of IBM Corporation, registered in many jurisdictions worldwide. SPSS is a trademark of SPSS Inc., an IBM Company, registered in many jurisdictions worldwide.

- ▶ Geben Sie in das Feld "Anmeldenenamen" Ihre Benutzer-ID ein.
- ▶ Geben Sie im Feld "Passwort" Ihr Passwort ein.
- ▶ Klicken Sie auf Anmelden. Standardmäßig wird die Seite "Konfiguration" angezeigt.

Weitere Optionen

Auf der Anmeldungsseite erhalten Sie auch die Möglichkeit, Ihr Passwort zu ändern. Für weitere Informationen siehe Thema [Ändern von Passwörtern](#) auf S. 14.

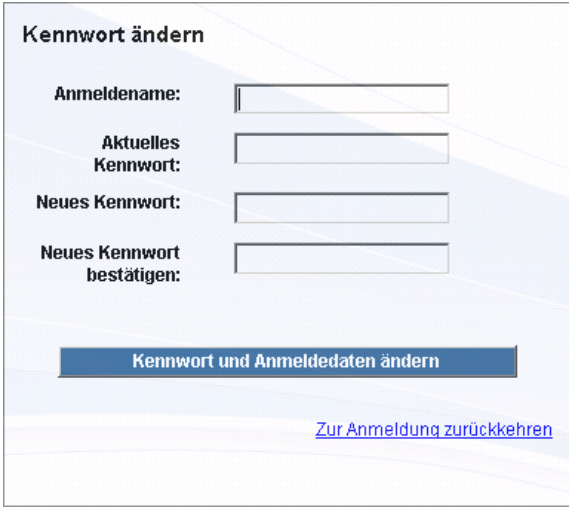
Wichtig: Einzelanmeldung ist für browserbasiertes IBM® SPSS® Collaboration and Deployment Services Deployment Manager nicht gestattet.

Ändern von Passwörtern

So ändern Sie Ihr Passwort:

Klicken Sie auf der Anmeldungsseite auf [Passwort ändern?](#) Das Dialogfeld "Passwort ändern" wird geöffnet.

Abbildung 3-2
Ändern Ihres Passworts



Kennwort ändern

Anmeldename:

Aktuelles Kennwort:

Neues Kennwort:

Neues Kennwort bestätigen:

Kennwort und Anmeldedaten ändern

[Zur Anmeldung zurückkehren](#)

- ▶ Geben Sie in das Feld “Anmeldenamen” Ihren Anmeldenamen ein.
- ▶ Geben Sie im Feld “Aktuelles Passwort” Ihr aktuelles Passwort ein.
- ▶ Geben Sie im Feld “Neues Passwort” Ihr neues Passwort ein.
- ▶ Wiederholen Sie im Feld “Neues Passwort bestätigen” Ihr neues Passwort.
- ▶ Klicken Sie auf Neues Passwort speichern. Im Abschnitt “Meldungen” wird der folgende Text angezeigt:
Passwort aktualisiert
- ▶ Klicken Sie auf Zur Anmeldung zurückkehren. Die Anmeldungsseite wird geöffnet. Melden Sie sich mit Ihrem neuen Passwort beim System an. Für weitere Informationen siehe Thema [Verwendung des browserbasierten IBM SPSS Collaboration and Deployment Services Deployment Manager](#) auf S. 13.

Navigation durch das browserbasierte IBM SPSS Collaboration and Deployment Services Deployment Manager

Das browserbasierte IBM® SPSS® Collaboration and Deployment Services Deployment Manager beruht primär auf der Navigation über Registerkarten. Im Allgemeinen sind Komponenten des Systems von Allgemein zu Spezifisch gegliedert. Im Navigationsbereich an der linken Seite können Sie beliebige der folgenden Kategorien wählen:

- Konfiguration
- Deployment Portal
- MIME-Typen
- Repository-Index
- Sicherheits-Provider

- Abmeldung
- Informationen zu
- Administratorhandbuch
- Hilfe

Mit jedem dieser Elemente sind einer oder mehr Abschnitte verknüpft. Wenn Sie auf ein Element klicken, wird der entsprechende Abschnitt im rechten Bereich angezeigt. Wenn ein Abschnitt über mehrere Unterabschnitte verfügt, wird eine Reihe von Registerkarten im rechten Fensterbereich angezeigt. Standardmäßig wird der Inhalt der ersten Registerkarte angezeigt. Wenn Sie beispielsweise in der Navigationsliste auf MIME-Typen klicken, wird der Bereich "MIME-Typen und Dateityp-Symbole" angezeigt.

Klicken auf "Festlegen" oder Drücken der Eingabetaste

Das System ist mausgesteuert. Es wird davon abgeraten, zum Fertigstellen von Aktionen die Eingabetaste zu drücken. In der Regel wird Ihre Anforderung durch das Drücken der Eingabetaste nicht übermittelt. Beispielsweise sehen Sie im ganzen System die Schaltfläche "Festlegen". Wenn Sie die Eingabetaste drücken anstatt auf Festlegen zu klicken, wird Ihre Anforderung nicht verarbeitet. Durch Klicken auf Festlegen werden Ihre Änderungen in die Datenbank geschrieben.

Zugriff auf Systeminformationen

Informationen zu Ihrer IBM® SPSS® Collaboration and Deployment Services-Installation können über die Info-Seite abgerufen werden. Die Seite zeigt die Versionsnummer für das System an und enthält außerdem die Informationen für individuelle Komponenten (installierte Pakete), darunter die allgemeine Komponentenkategorie ("Bereich"), Versionsnummer und Lizenz. Über diese Seite können Sie detaillierte Informationen zu den Dateien anzeigen, die in jedem Paket enthalten sind, und sie bietet die Möglichkeit, Systeminformationen, Installationsprotokolle und Anwendungsserverprotokolle herunterzuladen. Anwendungsserverprotokolle können zur Behebung von Fehlern im System verwendet werden. Für weitere Informationen siehe Thema [Fehlerbehebung](#) in Anhang A auf S. 133.

Anzeigen von detaillierten Informationen für installierte Pakete

- ▶ Klicken Sie auf Details anzeigen.

Herunterladen von Systeminformationen in Form einer Textdatei

- ▶ Klicken Sie auf Version und Systemdaten herunterladen am unteren Rand der Seite.

Herunterladen eines Zip-Archivs mit Versions- und Systeminformationen sowie dem Anwendungsserverprotokoll in Form von Textdateien

- ▶ Klicken Sie auf Version, Systemdetails und Protokolle als Zip-Datei herunterladen am unteren Rand der Seite. Die Datei wird als Zip-Archiv heruntergeladen.

Verwendung von IBM SPSS Collaboration and Deployment Services Deployment Manager

Verwaltungsaufgaben können sowohl mit dem IBM® SPSS® Collaboration and Deployment Services Deployment Manager als auch mit dem browserbasierten IBM® SPSS® Collaboration and Deployment Services Deployment Manager ausgeführt werden. Ein Administrator kann:

- Sicherheits-Provider konfigurieren und aktivieren.
- Benutzer und Gruppen für den Zugriff auf das System anlegen.
- Rollen zur Steuerung des Zugriffs auf Systemfunktionen definieren.

Zusätzlich erlaubt Deployment Manager die Administration anderer Server, etwa von IBM® SPSS® Statistics- und IBM® SPSS® Modeler-Servern.

Verwaltete Server

Die Server-Administration in IBM® SPSS® Collaboration and Deployment Services Deployment Manager umfasst:

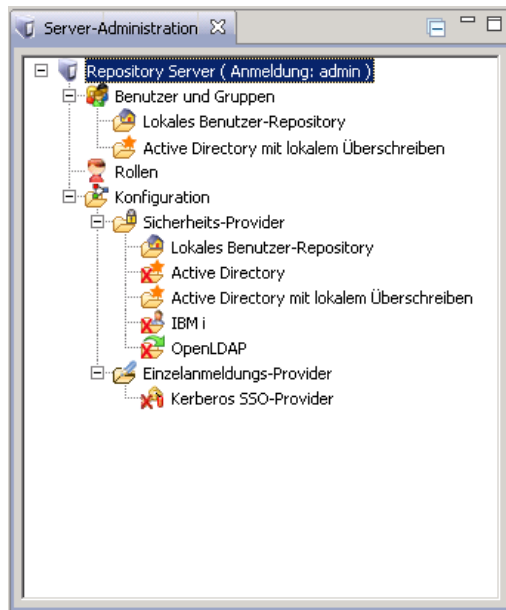
1. Hinzufügen des zu verwaltenden Servers zum System
2. Anmelden beim verwalteten Server
3. Bei Bedarf Ausführen von Administrationsaufgaben für den Server
4. Abmelden vom verwalteten Server

Die Registerkarte "Server-Administration" bietet Zugriff auf diese Funktionalität. Diese Registerkarte listet die Server auf, die derzeit verwaltet werden können. Diese Liste bleibt über Deployment Manager-Sitzungen hinweg bestehen und vereinfacht den Zugriff auf diese Server.

Wählen Sie die folgenden Befehle aus den Menüs aus:

Werkzeuge > Server-Administration

Abbildung 3-3
Liste der verwalteten Server



Die Liste verwalteter Server kann verschiedenen Servertypen enthalten, z. B. IBM® SPSS® Collaboration and Deployment Services Repository-Server, IBM® SPSS® Modeler-Server und IBM® SPSS® Statistics-Server. Die tatsächlichen Verwaltungsfunktionen, die für einen Server verfügbar sind, hängen vom Servertyp ab. Sicherheits-Provider können beispielsweise für Repository-Server, jedoch nicht für SPSS Modeler-Server konfiguriert und aktiviert werden.

Hinzufügen von neuen verwalteten Servern

Vor dem Ausführen von Administrationsaufgaben muss eine Verbindung zum verwalteten Server aufgebaut werden.

Wählen Sie die folgenden Befehle aus den Menüs aus:

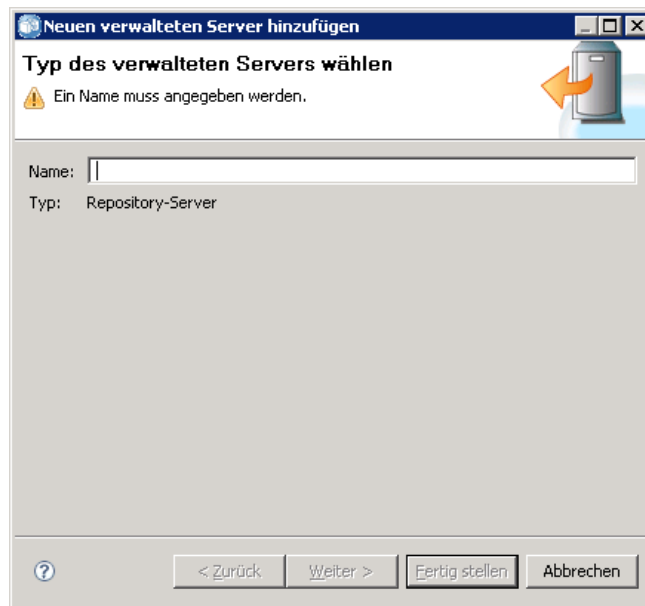
Datei > Neu > Verwaltete Server-Verbindung

Das Dialogfeld "Neuen verwalteten Server hinzufügen" wird geöffnet. Beim Hinzufügen einer neuen Verbindung müssen der Typ des verwalteten Servers und die Informationen zum verwalteten Sicherheitsserver angegeben werden.

Auswählen von Name und Typ des verwalteten Servers

Der erste Schritt beim Hinzufügen eines verwalteten Servers zum System besteht darin, zwei Parameter für den Server zu definieren: den Namen und den Typ.

Abbildung 3-4
Dialogfeld "Typ des verwalteten Servers wählen"



Name. Ein Label, mit dessen Hilfe der vorherige Server auf der Registerkarte "Server-Administration" identifiziert wird. Die Angabe der Portnummer, z. B. *my_server:8080*, kann helfen, den Server in der Liste der verwalteten Server zu identifizieren.

Hinweis: Alphanumerische Zeichen werden empfohlen. Folgende Zeichen sind verboten:

- Anführungszeichen (einfach und doppelt)
- Ampersands (&)
- Kleiner-als- (<) und Größer-als-Zeichen (>)
- Periods
- Kommas
- Semikolons

Typ. Typ des Servers, der hinzugefügt wird. Die Liste der möglichen Servertypen hängt von der Systemkonfiguration ab. Möglich sind:

- IBM® SPSS® Collaboration and Deployment Services Repository Server
- Verwaltete IBM® SPSS® Modeler-Server
- Verwaltete IBM® SPSS® Statistics-Server
- Verwaltete IBM® SPSS® Text Analytics-Server

Auswählen des Typs eines verwalteten Servers

Gehen Sie im Dialogfeld "Typ des verwalteten Servers wählen" wie folgt vor:

1. Geben Sie einen Namen für den Server ein.

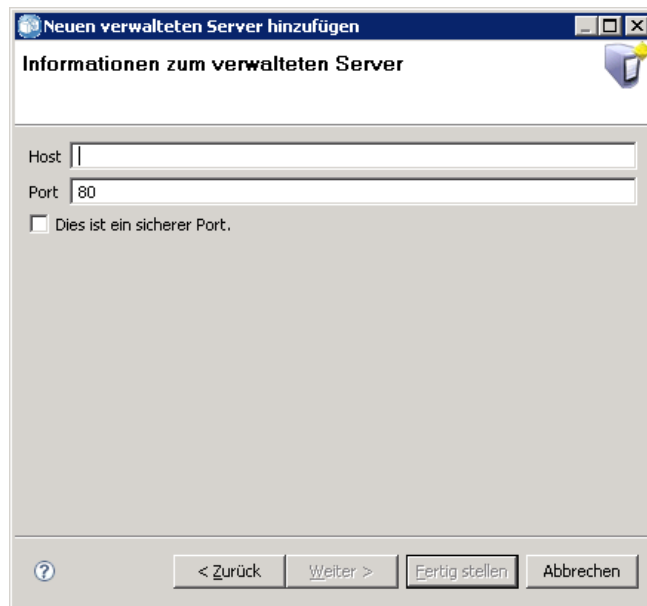
2. Wählen Sie den Servertyp aus.
3. Klicken Sie auf Weiter. Das Dialogfeld “Informationen zum verwalteten Sicherheitsserver” wird geöffnet.

Informationen zum verwalteten Server

Der zweite Schritt beim Hinzufügen eines verwalteten Servers zum System besteht in der Definition der Servereigenschaften.

Abbildung 3-5

Dialogfeld “Informationen zum verwalteten Sicherheitsserver”



Host. Der Name bzw. die IP-Adresse des Servers.

Hinweis: Alphanumerische Zeichen werden empfohlen. Folgende Zeichen sind verboten:

- Anführungszeichen (einfach und doppelt)
- Ampersands (&)
- Kleiner-als- (<) und Größer-als-Zeichen (>)
- Periods
- Kommas
- Semikolons

Port. Die Portnummer für die Server-Verbindung.

Dies ist ein sicherer Port. Aktiviert oder deaktiviert die Verwendung eines Secure Sockets Layer (SSL) für die Server-Verbindung. Diese Option ist nicht für alle Typen von verwalteten Servern verfügbar.

Angeben von Informationen zum verwalteten Server

Gehen Sie im Dialogfeld “Informationen zum verwalteten Sicherheitsserver” wie folgt vor:

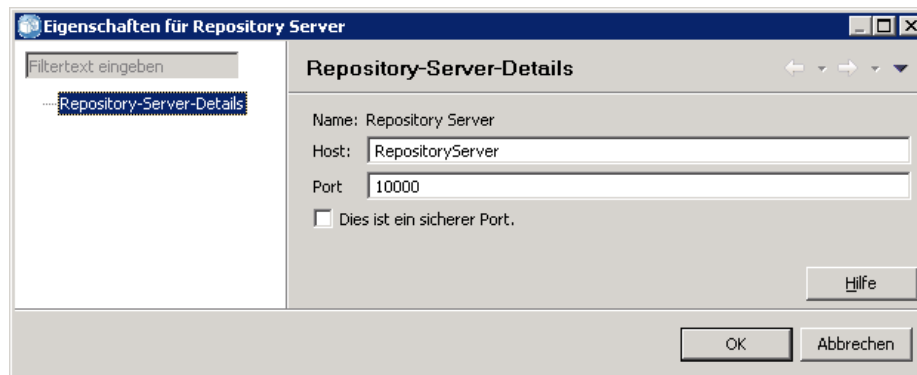
1. Geben Sie den Hostnamen oder die IP-Adresse des Servers ein, der hinzugefügt wird.
2. Geben Sie die Portnummer an, an der der hinzugefügte Server ausgeführt werden soll.
3. Geben Sie an, ob der Server SSL verwendet, falls zutreffend.
4. Klicken Sie auf Fertig stellen.

Der Server wird in der Liste der verwalteten Server auf der Registerkarte “Server-Administration” angezeigt.

Anzeigen von Eigenschaften des verwalteten Servers

Um die Eigenschaften eines bestehenden verwalteten Servers anzuzeigen, klicken Sie mit der rechten Maustaste auf die Registerkarte “Server-Administration” und wählen Sie Eigenschaften aus dem Dropdown-Menü. Das Dialogfeld Eigenschaften wird geöffnet. Die angezeigten Eigenschaften hängen vom Typ des ausgewählten Servers ab.

Abbildung 3-6
IBM SPSS Collaboration and Deployment Services Repository-Server-Eigenschaften



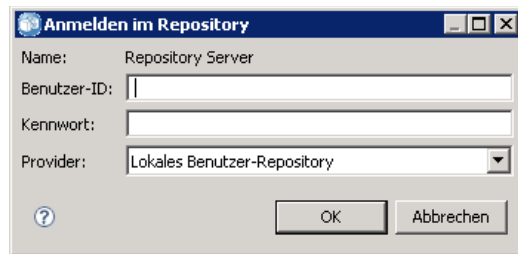
Eigenschaften für Repository-Server:

- **Bezeichnung.** Der mit dem Server verbundene Name, wie er in der Registerkarte “Server-Administration” angezeigt wird.
- **Host.** Der Name bzw. die IP-Adresse des Servers.
- **Port.** Die Portnummer für die Server-Verbindung.
- **Dies ist ein sicherer Port.** Wenn diese Option ausgewählt ist, verwendet der Server eine SSL-Verbindung für die Kommunikation.

Verbinden mit verwalteten Servern

Für die meisten Server müssen Sie die Verbindung in der Liste der verwalteten Server herstellen, um Verwaltungsaufgaben auszuführen. Doppelklicken Sie in der Registerkarte “Server-Administration” auf den Server, den Sie verwalten möchten. Das Dialogfeld “Anmelden beim Server” wird geöffnet.

Abbildung 3-7
Dialogfeld “Anmelden beim Server”



Anmeldeparameter für Repository-Server:

Benutzer-ID. Der Benutzer, der sich am Server anmelden möchte, in Klartext.

Paßwort. Die Zeichenfolge, die zur Authentifizierung des Benutzers verwendet wird. Aus Sicherheitsgründen wird der Passworttext maskiert dargestellt.

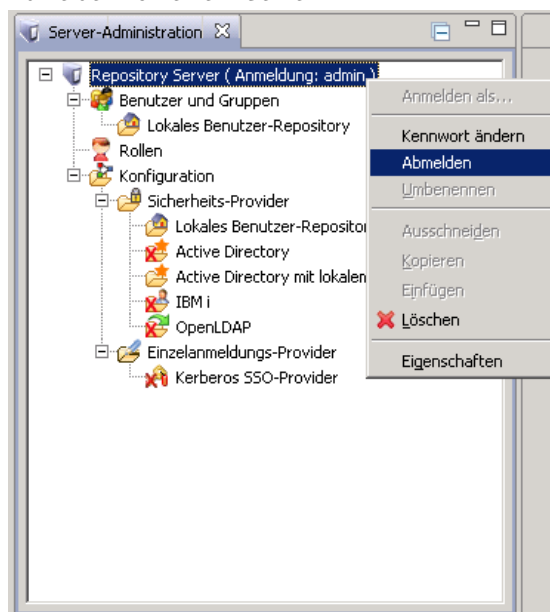
Anbieter. Der Provider, für den die angegebene Anmeldung-Passwort-Kombination geprüft werden muss. Dieses Feld wird nur angezeigt, wenn mehrere Sicherheits-Provider für das System aktiviert sind. Andernfalls validiert das System die angegebenen Anmeldedaten im lokalen Benutzer-Repository.

Trennen der Verbindung zu verwalteten Servern

Nach Erledigung der gewünschten Verwaltungsaufgaben melden Sie sich vom Server ab.

1. Klicken Sie in der Registerkarte “Server-Administration” mit der rechten Maustaste auf den Server.
2. Wählen Sie Abmelden.

Abbildung 3-8
Abmelden von einem Server



Um den Server wieder zu verwalten, müssen Sie sich erneut anmelden.

Löschen von verwalteten Servern

Ein Server wird in der Liste der verwalteten Server angezeigt, bis er aus der Liste gelöscht wird.

1. Wählen Sie in der Registerkarte "Server-Administration" den Server aus, den Sie löschen möchten.
2. Wählen Sie die folgenden Befehle aus den Menüs aus:
Bearbeiten > Löschen

Oder klicken Sie mit der rechten Maustaste auf den Server und wählen Sie Löschen aus dem Dropdown-Menü.

Wenn weitere Verwaltungsaufgaben für den Server erledigt werden müssen, muss der Server dem System erneut hinzugefügt werden.

Namenskonventionen

Überall im System werden Sie aufgefordert, Entitäten von Ordnern bis Themen zu benennen. Beispielsweise könnten Sie einen neuen Benutzer hinzufügen oder ein neues Thema erstellen.

Es gelten die folgenden Namenskonventionen:

- Die meisten Zeichen, einschließlich Leerzeichen, werden vom System akzeptiert. Nur der Schrägstrich (/) ist nicht erlaubt. Wenn Sie den Schrägstrich als Teil eines Namens eingeben, wird dieser nicht in den Namen aufgenommen.

- Die maximale Länge beträgt 255 Zeichen, einschließlich Leerzeichen.
- Bei den Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Benutzer und Gruppen

Ein IBM® SPSS® Collaboration and Deployment Services-Benutzer ist eine Person oder ein Prozess mit der Erlaubnis, auf Dateien zuzugreifen und Programme auszuführen. Der Benutzer wird mit einem Benutzernamen-Passwort-Paar an einer internen oder externen Datenbank verifiziert. Benutzer verfügen über unterschiedliche Zugriffsebenen für Anwendungsressourcen.

Benutzer können auf der Basis von ihrem Bedarf an Informationszugriff und -änderung in Gruppen organisiert werden. Das Einteilen von Benutzern in Gruppen kann den Aufwand minimieren, der für die einheitliche und strukturierte Verteilung von Berechtigungen an mehrere Benutzer erforderlich wäre.

Benutzer und Gruppen wird der Zugriff auf Systemressourcen mithilfe von *Rollen* zugewiesen. Eine Rolle umfasst eine Gruppe von Aktionen, die im System vordefiniert sind, z. B. Zugriff auf Dateien und MIME-Typen, Ändern der Systemkonfiguration usw. Rollenzuordnungen können hinzugefügt oder entfernt werden, und bei geänderten Anforderungen können neue Rollen erstellt werden. Beachten Sie, dass Rollen explizit zugewiesen werden müssen, bevor Benutzer auf das System zugreifen können. Für weitere Informationen siehe Thema [Überblick über Rollen](#) in Kapitel 5 auf S. 40.

IBM SPSS Collaboration and Deployment Services-Benutzer und -Gruppen werden von *Sicherheits-Providern* verwaltet. Ein Sicherheits-Provider ist das System, das die Benutzeranmeldedaten authentifiziert. Benutzer und Gruppen können lokal definiert werden (in diesem Fall ist IBM SPSS Collaboration and Deployment Services der Sicherheits-Provider) oder aus einem Remote-Verzeichnis wie Windows Active Directory oder OpenLDAP abgeleitet werden. Für weitere Informationen siehe Thema [Sicherheits-Provider](#) in Kapitel 6 auf S. 48.

Manche Umgebungen erfordern eventuell das Einrichten von Gruppen aus remote definierten Benutzern, die für IBM® SPSS® Collaboration and Deployment Services Deployment Manager spezifisch sind. Dies ist der Fall, wenn Gruppen, die im Remote-Verzeichnis angegeben sind, nicht differenziert genug sind. Der Verzeichnis-Administrator ist eventuell nicht in der Lage, diese spezifischeren Gruppen zu erstellen, weil Richtlinienbeschränkungen bestehen oder Abfragen des Remote-Verzeichnisses von externen Anwendungen nicht erlaubt sind. In diesen Fällen werden lokal angegebene Gruppen von Remote-Benutzern, sogenannte *erweiterte Gruppen*, der Liste der bereits im Remote-Verzeichnis definierten Gruppen hinzugefügt.

In vielen Umgebungen ist die Anzahl der Benutzer in einem Remote-Verzeichnis ziemlich hoch, während nur eine kleine Untergruppe des gesamten Benutzerpools Zugriff auf IBM SPSS Collaboration and Deployment Services benötigt. In diesem Fall kann der Administrator eine Liste von *erlaubten Benutzern* angeben, und nur diese Benutzer dürfen sich anmelden. Die Liste mit erlaubten Benutzern fungiert als Filter für den Benutzernamen, aber die eigentliche Authentifizierung des Benutzers wird auf normale Weise am Remote-Directory ausgeführt.

Einrichten von IBM SPSS Collaboration and Deployment Services-Benutzern

Das Setup von lokalen Benutzern in IBM® SPSS® Collaboration and Deployment Services umfasst:

1. Erstellen des Benutzers und ggf. Zuweisung der Gruppenmitgliedschaft. Lokale Benutzer und Gruppen können durch IBM® SPSS® Collaboration and Deployment Services Deployment Manager verwaltet werden.
2. Das Definieren der Zugriffsebene für den Benutzer durch Zuweisen der Rolle auf Benutzer- oder Gruppenbasis. Für weitere Informationen siehe Thema [Bearbeiten von Benutzern und Gruppen, die einer Rolle zugewiesen sind](#) in Kapitel 5 auf S. 45. Wenn die Rolle mit den geeigneten festgelegten Aktionen nicht existiert, muss sie eingerichtet werden. Für weitere Informationen siehe Thema [Erstellen einer neuen Rolle](#) in Kapitel 5 auf S. 43.

Das Setup von extern definierten Benutzern in IBM SPSS Collaboration and Deployment Services umfasst:

1. Einrichten des externen Sicherheits-Providers, falls dieser noch nicht definiert wurde. Der Benutzer wird aus diesem Sicherheits-Provider abgeleitet. Für weitere Informationen siehe Thema [Konfigurieren von Sicherheits-Providern](#) in Kapitel 6 auf S. 49.
2. Das Erstellen erlaubter Benutzer, wenn der Zugriff auf einen untergeordneten Bereich des Active Directory auf +lokal überschriebene Benutzer beschränkt werden muss. Erlaubte Benutzer können nur mit Deployment Manager erstellt werden.
3. Das Definieren der erweiterten Gruppe und das Hinzufügen des Benutzers zur Gruppe, wenn der lokal überschriebene Benutzer einer Gruppe zugewiesen werden muss, die nicht im Remote-Verzeichnis existiert. Erweiterte Gruppen können nur mit Deployment Manager erstellt werden.
4. Zuweisen der Rolle auf Benutzer- oder Gruppenbasis. Rollen werden remote definierten Benutzern auf dieselbe Weise wie lokalen Benutzern zugewiesen.

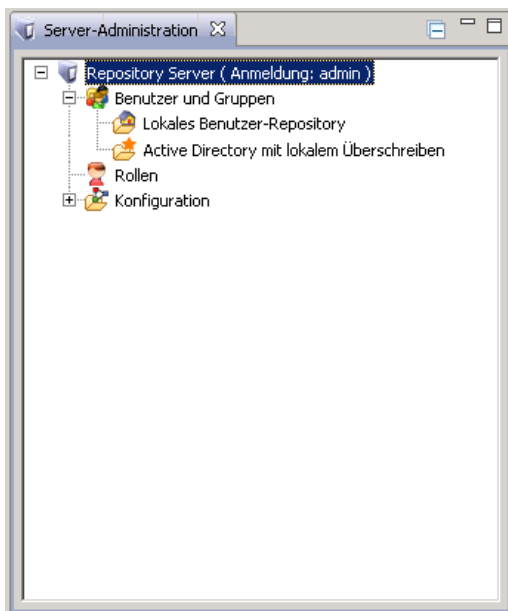
Verwalten von Benutzern und Gruppen in IBM SPSS Collaboration and Deployment Services Deployment Manager

IBM® SPSS® Collaboration and Deployment Services Deployment Manager ermöglicht Ihnen, lokale Benutzer und Gruppen sowie erlaubte Benutzer und erweiterte Gruppen zu verwalten, die für das Active Directory mit lokal überschriebenem Sicherheits-Provider definiert sind. Bevor Sie Aktionen mit Benutzern oder Gruppen ausführen, navigieren Sie zur administrativen Schnittstelle, die diese Bereiche steuert.

1. Wählen Sie im Menü “Extras” die Server-Administration.
2. Melden Sie sich in der Registerkarte “Server-Administration” bei einem IBM® SPSS® Collaboration and Deployment Services Repository-Server an. Doppelklicken Sie auf das Symbol Benutzer und Gruppen, um die Hierarchie zu erweitern. Wenn keine externen Sicherheits-Provider eingerichtet sind, ist “Lokales Benutzer-Repository” der einzige Eintrag in der Hierarchie. Wenn

Active Directory mit lokalem Überschreiben als Sicherheits-Provider mit der Option für erlaubte Benutzer oder erweiterte Gruppen konfiguriert wurde, wird auch der Eintrag “Active Directory mit lokalem Überschreiben” angezeigt.

Abbildung 4-1
Registerkarte “Server-Administration”

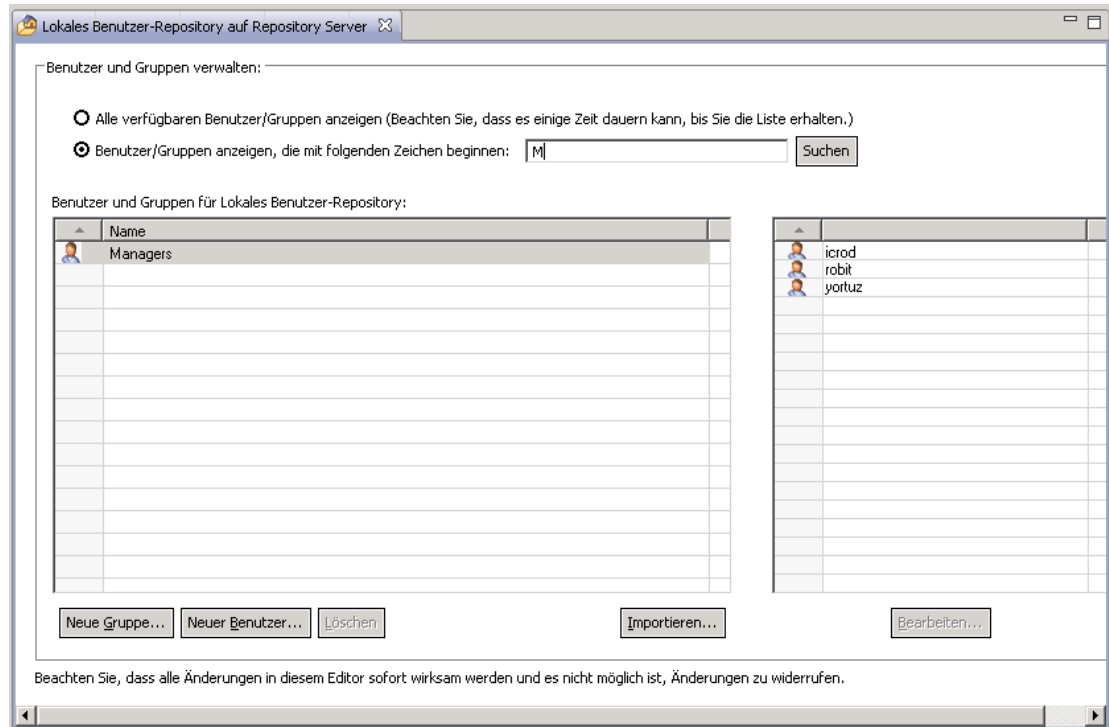


3. Doppelklicken Sie auf das Symbol Lokales Benutzer-Repository oder Active Directory mit lokalem Überschreiben.

Der Editor “Benutzer und Gruppen verwalten” wird geöffnet.

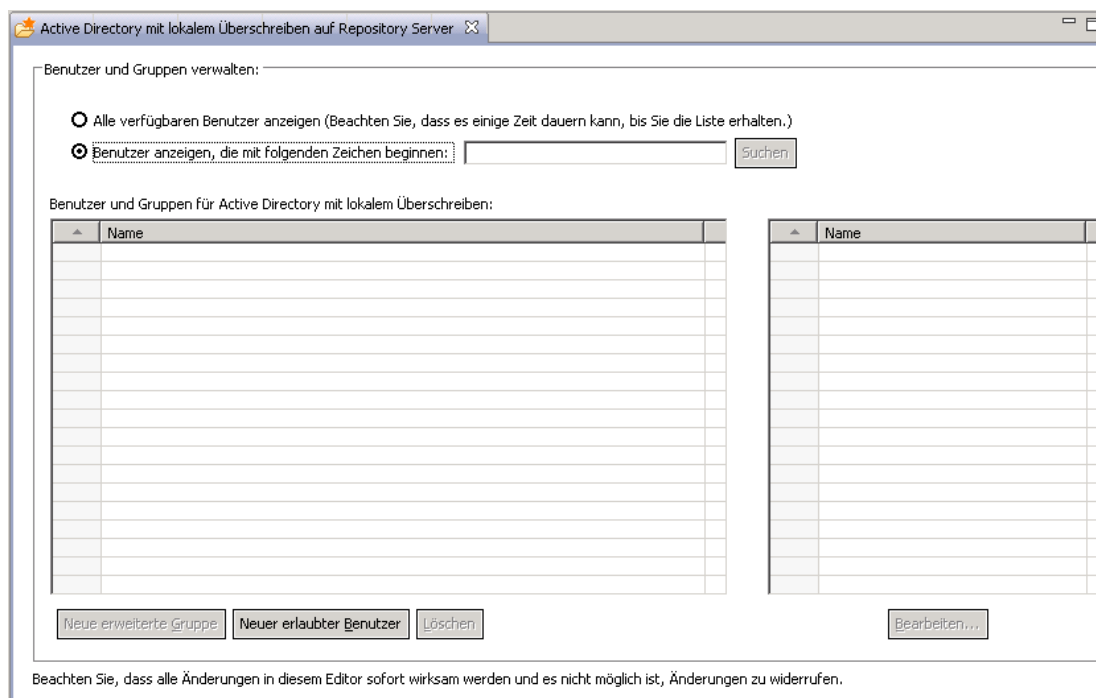
- Für “Lokales Benutzer-Repository” zeigt der Editor alle nativen Benutzer und Gruppen oder eine gefilterte Liste auf der Basis der Anfangsbuchstaben in den Benutzer- und Gruppennamen. Ein Administrator kann Benutzer und Gruppen erstellen und löschen, die Eigenschaften von bestehenden Benutzern und Gruppen bearbeiten sowie Benutzer und Gruppen importieren.

Abbildung 4-2
Editor "Benutzer und Gruppen verwalten"



- Für "Active Directory mit lokalem Überschreiben" zeigt der Editor alle extern definierten Gruppen und Benutzer an, die für den Zugriff auf IBM® SPSS® Collaboration and Deployment Services eingerichtet wurden, oder eine gefilterte Liste auf der Basis der Anfangsbuchstaben in den Benutzer- und Gruppennamen. Ein Administrator kann erlaubte Benutzer und erweiterte Gruppen erstellen und löschen und die Eigenschaften von bestehenden Gruppen bearbeiten, wenn die Optionen für erlaubte Benutzer und erweiterte Gruppen für den Sicherheits-Provider aktiviert sind. Für weitere Informationen siehe Thema [Sicherheits-Provider](#) in Kapitel 6 auf S. 48.

Abbildung 4-3
Editor "Benutzer und Gruppen verwalten" für Active Directory mit lokalem Überschreiben



Erstellen eines Benutzers

Klicken Sie im Editor "Benutzer und Gruppen verwalten" für "Lokales Benutzer-Repository" auf Neuer Benutzer. Das Dialogfeld "Neuen Benutzer erstellen" wird geöffnet.

Abbildung 4-4
Dialogfeld "Neuen Benutzer erstellen"

Benutzername. Der Name unterscheidet keine Groß-/Kleinschreibung und kann Leerzeichen enthalten.

Paßwort. Das Passwort des lokalen Benutzers. Beim Passwort wird zwischen Groß- und Kleinschreibung unterschieden.

Bestätigen. Feld zur Bestätigung des Passworts. Wenn die Passwörter nicht übereinstimmen, wird eine Meldung angezeigt.

Alle verfügbaren Gruppen anzeigen. Gibt eine Liste aller vom System erkannten Gruppen zurück. Beachten Sie, dass für sehr umfangreiche Verzeichnisse eventuell die Anzahl der Einträge, die angezeigt werden können, beschränkt ist. Daher wird die Angabe eines Suchstrings empfohlen.

Gruppen anzeigen, die mit folgenden Zeichen beginnen. Filtert die Liste mit den verfügbaren Gruppen gemäß dem eingegebenen String. Verwenden Sie dieses Feld, um die Liste der verfügbaren Gruppen auszuarbeiten.

Verfügbare Gruppen. Listet die erkannten Gruppen auf, denen der Benutzer zugewiesen werden kann.

Benutzer gehört zu Gruppen. Listet die Gruppen auf, denen der Benutzer derzeit zugewiesen ist.

Alle hinzufügen. Assoziiert alle Gruppen mit dem Benutzer.

Alle entfernen. Entfernt alle angezeigten Gruppen vom Benutzer.

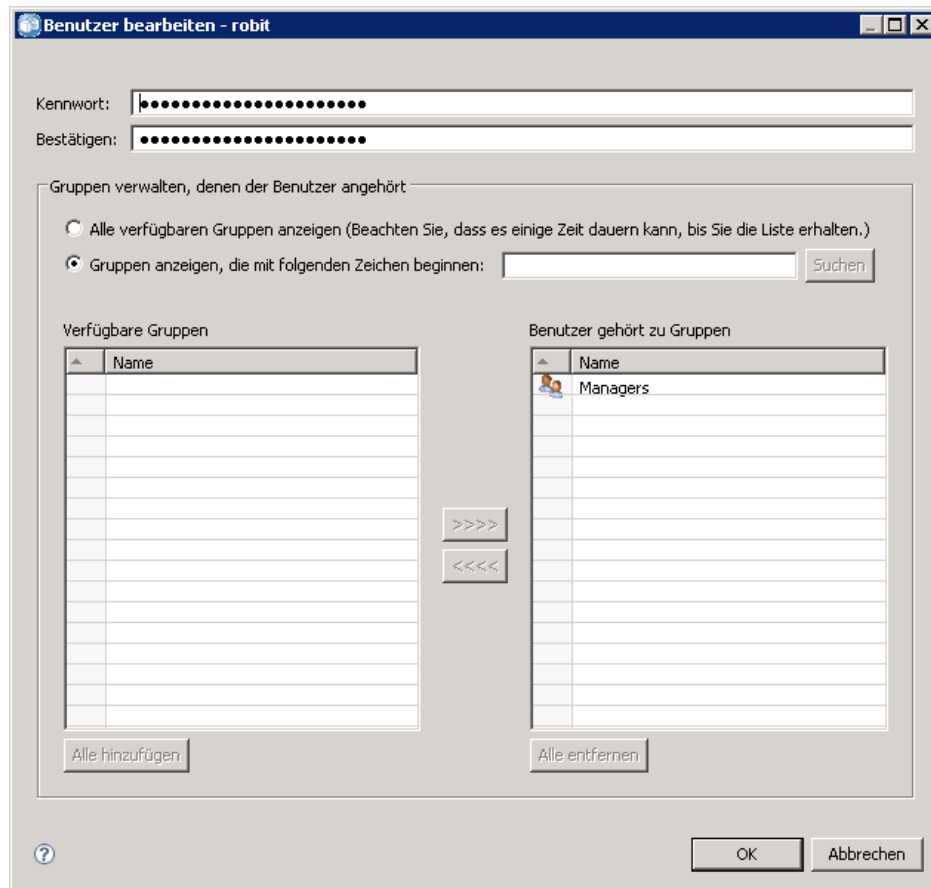
Für das Erstellen eines lokalen Benutzers müssen Anmeldedaten angegeben werden. Der Benutzer kann außerdem mit Gruppen assoziiert werden.

1. Geben Sie im Dialogfeld "Neuen Benutzer erstellen" den Benutzernamen ein.
2. Geben Sie das Passwort ein.
3. Bestätigen Sie das Passwort.
4. Assoziieren Sie den Benutzer bei Bedarf mit Gruppen.
5. Klicken Sie auf OK. Der neue Benutzer erscheint in der Liste im Editor "Benutzer und Gruppen verwalten".

Bearbeiten eines Benutzers

Gruppenzuordnungen können für lokale und erlaubte Benutzer in Active Directory mit lokalem Überschreiben bearbeitet werden. Für lokale Benutzer kann das Passwort ebenfalls bearbeitet werden. Wählen Sie im Editor "Benutzer und Gruppen verwalten" den Benutzer aus und klicken Sie auf Bearbeiten. Das Dialogfeld "Benutzer bearbeiten" wird geöffnet.

Abbildung 4-5
Dialogfeld "Benutzer bearbeiten"



Paßwort. Das Passwort des lokalen Benutzers. Beim Passwort wird zwischen Groß- und Kleinschreibung unterschieden.

Bestätigen. Feld zur Bestätigung des Passworts. Wenn die Passwörter nicht übereinstimmen, wird eine Meldung angezeigt.

Alle verfügbaren Gruppen anzeigen. Gibt eine Liste aller vom System erkannten Gruppen zurück. Beachten Sie, dass für sehr umfangreiche Verzeichnisse eventuell die Anzahl der Einträge, die angezeigt werden können, beschränkt ist. Daher wird die Angabe eines Suchstrings empfohlen.

Gruppen anzeigen, die mit folgenden Zeichen beginnen. Filtert die Liste mit den verfügbaren Gruppen gemäß dem eingegebenen String. Verwenden Sie dieses Feld, um die Liste der verfügbaren Gruppen auszuarbeiten.

Verfügbare Gruppen. Listet die erkannten Gruppen auf, denen der Benutzer zugewiesen werden kann.

Benutzer gehört zu Gruppen. Listet die Gruppen auf, denen der Benutzer derzeit zugewiesen ist.

Alle hinzufügen. Assoziiert alle Gruppen mit dem Benutzer.

Alle entfernen. Entfernt alle angezeigten Gruppen vom Benutzer.

Löschen eines Benutzers

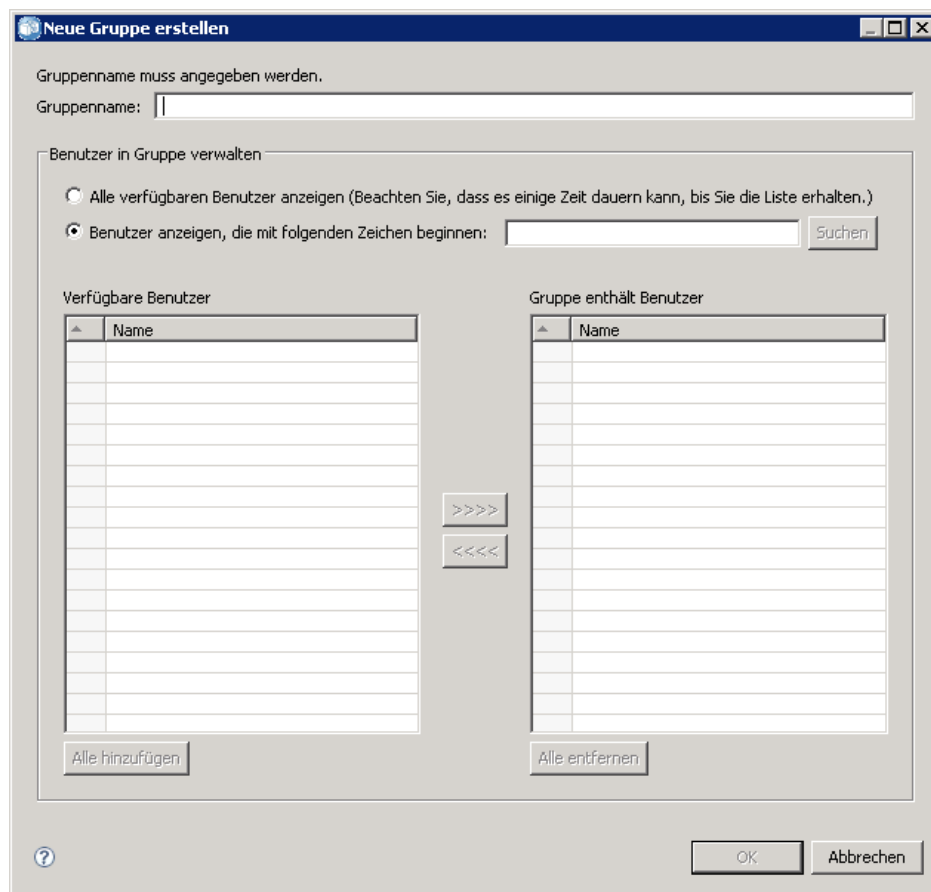
So löschen Sie einen lokalen Benutzer oder einen erlaubten Benutzer in Active Directory mit lokalem Überschreiben:

1. Wählen Sie den Benutzer im Editor “Benutzer und Gruppen verwalten” aus.
2. Klicken Sie auf die Schaltfläche Löschen. Ein Dialogfeld wird geöffnet, in dem Sie bestätigen können, dass der Benutzer gelöscht werden soll.
3. Klicken Sie auf Ja, um den Benutzer aus dem System zu löschen. Der Benutzer wird aus der Liste “Benutzer/Gruppe” gelöscht.

Erstellen einer Gruppe

Klicken Sie im Editor “Benutzer und Gruppen verwalten” für “Lokales Benutzer-Repository” auf Neue Gruppe. Das Dialogfeld “Neue Gruppe erstellen” wird geöffnet.

Abbildung 4-6
Dialogfeld “Neue Gruppe erstellen”



Gruppenname. Der Name unterscheidet keine Groß-/Kleinschreibung und kann Leerzeichen enthalten.

Alle verfügbaren Benutzer anzeigen. Gibt eine Liste aller vom System erkannten Benutzer zurück. Beachten Sie, dass für sehr umfangreiche Verzeichnisse eventuell die Anzahl der Einträge, die angezeigt werden können, beschränkt ist. Daher wird die Angabe eines Suchstrings empfohlen.

Benutzer anzeigen, die mit folgenden Zeichen beginnen. Filtert die Liste mit den verfügbaren Gruppen gemäß dem eingegebenen String. Verwenden Sie dieses Feld, um die Liste der verfügbaren Gruppen auszuarbeiten.

Verfügbare Benutzer. Listet die erkannten Benutzer auf, die der Gruppe hinzugefügt werden können.

Gruppe enthält Benutzer. Listet die Benutzer auf, die der Gruppe zugewiesen sind.

Alle hinzufügen. Assoziiert alle Benutzer mit der Gruppe.

Alle entfernen. Entfernt alle angezeigten Benutzer aus der Gruppe.

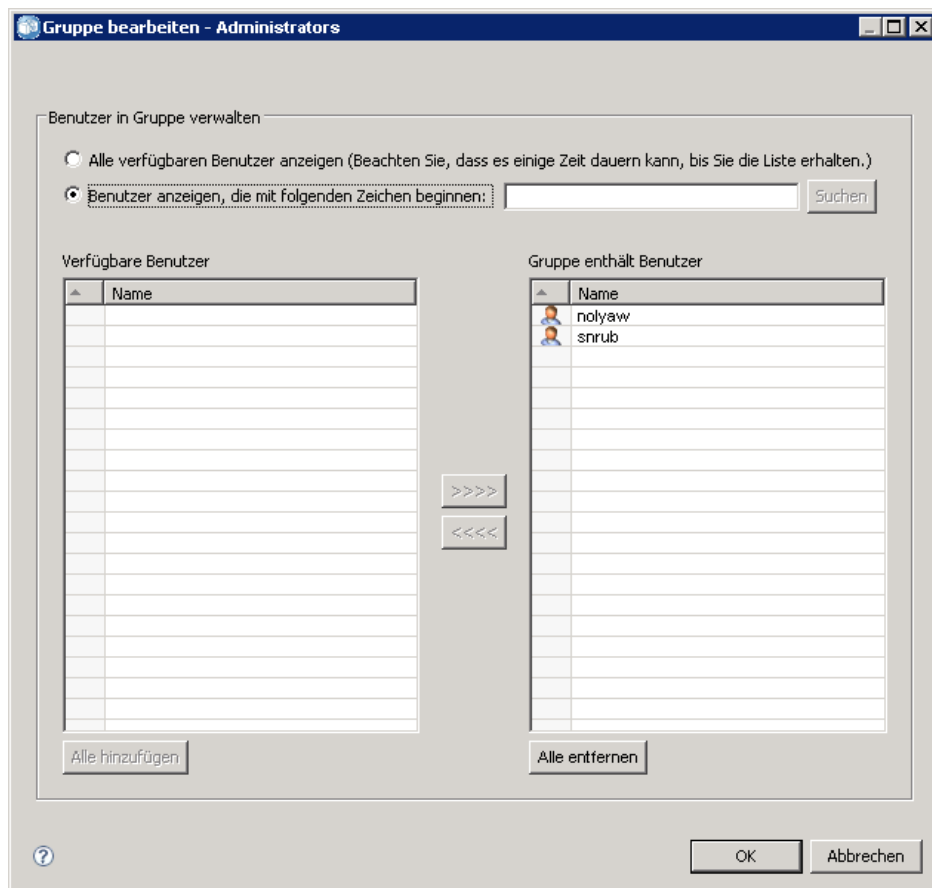
Für das Erstellen einer lokalen Gruppe muss der Benutzername angegeben werden. Der Gruppe können auch Benutzer hinzugefügt werden.

1. Geben Sie den Gruppennamen an.
2. Fügen Sie der Gruppe bei Bedarf Benutzer hinzu.
3. Klicken Sie auf OK. Die neue Gruppe erscheint in der Liste im Editor "Benutzer und Gruppen verwalten".

Bearbeiten einer Gruppe

Die Benutzerliste kann für lokale Gruppen und erweiterte Gruppen in Active Directory mit lokalem Überschreiben geändert werden. Wählen Sie im Editor "Benutzer und Gruppen verwalten" eine Gruppe aus und klicken Sie auf Bearbeiten. Das Dialogfeld "Gruppe bearbeiten" wird geöffnet.

Abbildung 4-7
Dialogfeld "Gruppe bearbeiten"



Alle verfügbaren Benutzer anzeigen. Gibt eine Liste aller vom System erkannten Benutzer zurück. Beachten Sie, dass für sehr umfangreiche Verzeichnisse eventuell die Anzahl der Einträge, die angezeigt werden können, beschränkt ist. Daher wird die Angabe eines Suchstrings empfohlen.

Benutzer anzeigen, die mit folgenden Zeichen beginnen. Filtert die Liste mit den verfügbaren Gruppen gemäß dem eingegebenen String. Verwenden Sie dieses Feld, um die Liste der verfügbaren Gruppen auszuarbeiten.

Verfügbare Benutzer. Listet die erkannten Benutzer auf, die der Gruppe hinzugefügt werden können.

Gruppe enthält Benutzer. Listet die Benutzer auf, die der Gruppe zugewiesen sind.

Alle hinzufügen. Assoziiert alle Benutzer mit der Gruppe.

Alle entfernen. Entfernt alle angezeigten Benutzer aus der Gruppe.

Löschen einer Gruppe

So löschen Sie eine lokale Gruppe oder eine erweiterte Gruppe in Active Directory mit lokalem Überschreiben:

1. Wählen Sie die zu löschende Gruppe im Editor “Benutzer und Gruppen verwalten” aus.
2. Klicken Sie auf die Schaltfläche Löschen. Ein Dialogfeld wird geöffnet, in dem Sie bestätigen können, dass der Eintrag gelöscht werden soll.
3. Klicken Sie auf Ja, um ihn aus dem System zu löschen. Die Gruppe wird aus der Liste “Benutzer/Gruppe” gelöscht.

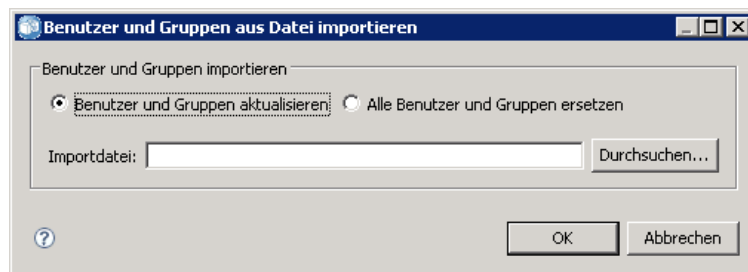
Importieren von Benutzern und Gruppen

Wenn Sie eine große Anzahl an lokalen Benutzern und Gruppen definieren müssen, können Sie mithilfe einer Principals-Importdatei Benutzer und Gruppen in großem Umfang importieren. Diese Datei muss die Struktur einhalten, die im Schema *nativestore.xsd* definiert ist. Weitere Informationen finden Sie unter [Anhang B](#).

So importieren Sie Benutzer und Gruppen:

1. Klicken Sie im Editor “Benutzer und Gruppen verwalten” für “Lokales Benutzer-Repository” auf die Schaltfläche Importieren. Das Dialogfeld Benutzer und Gruppen aus Datei importieren wird geöffnet.

Abbildung 4-8
Dialogfeld “Benutzer und Gruppen aus Datei importieren”

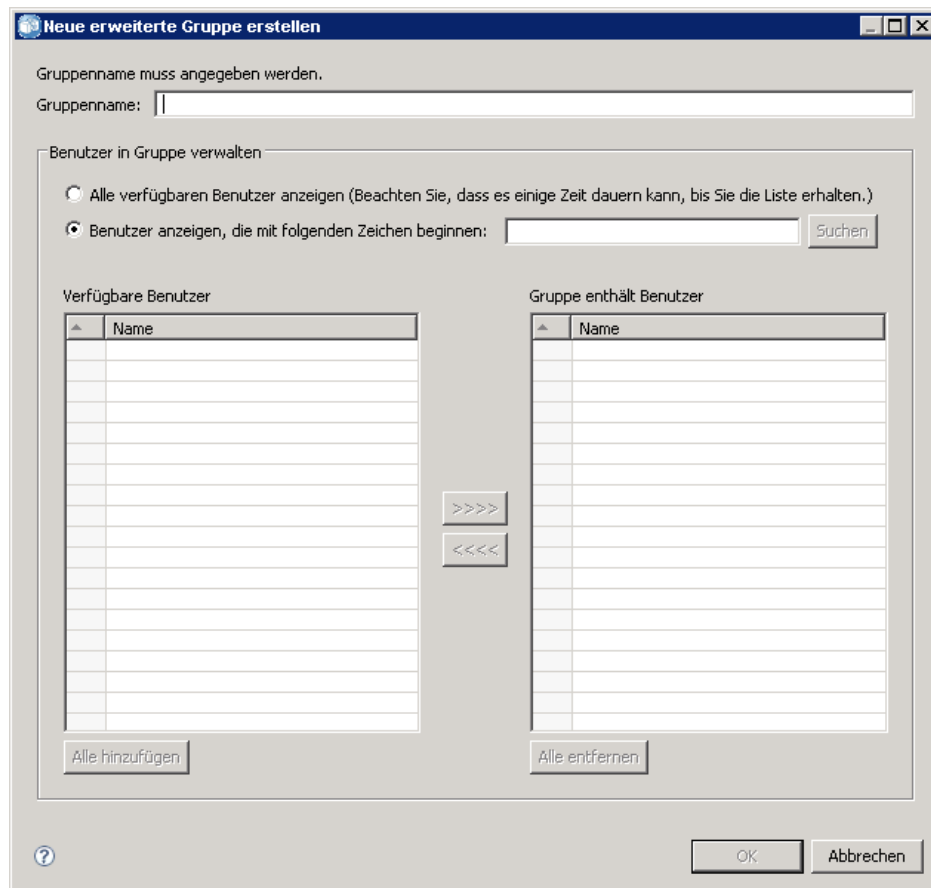


2. Wählen Sie Benutzer und Gruppen aktualisieren oder Alle Benutzer und Gruppen ersetzen.
 - **Benutzer und Gruppen aktualisieren.** Aktualisiert die bestehenden Benutzer und Gruppen mit den Informationen aus der Importdatei. Bestehende Benutzer und Gruppen, die nicht in der Datei definiert sind, werden nicht aktualisiert.
 - **Benutzer und Gruppen ersetzen.** Ersetzt die aktuellen Benutzer und Gruppen durch die Informationen aus der Importdatei. Bestehende Benutzer und Gruppen, die nicht in der Datei definiert sind, werden entfernt.
3. Navigieren Sie zum Speicherort der Importdatei.
4. Klicken Sie auf OK, um die Datei zu importieren. Die neuen Benutzer und Gruppen erscheinen in der Liste im Editor “Benutzer und Gruppen verwalten”.

Erstellen einer erweiterten Gruppe

Klicken Sie im Editor “Benutzer und Gruppen verwalten” für “Active Directory mit lokalem Überschreiben” auf Neue erweiterte Gruppe. Das Dialogfeld “Neue erweiterte Gruppe erstellen” wird geöffnet.

Abbildung 4-9
Dialogfeld “Neue erweiterte Gruppe erstellen”



Alle verfügbaren Benutzer anzeigen. Wenn die Option “Erlaubte Benutzer” aktiviert ist, wird die Liste aller erlaubten Benutzer zurückgegeben. Wenn die Option “Erlaubte Benutzer” nicht aktiviert ist, wird eine Liste mit allen Benutzern im Verzeichnis zurückgegeben. Beachten Sie, dass für sehr umfangreiche Verzeichnisse eventuell die Anzahl der Einträge, die angezeigt werden können, beschränkt ist. Daher wird die Angabe eines Suchstrings empfohlen.

Benutzer anzeigen, die mit folgenden Zeichen beginnen. Filtert die Liste mit den verfügbaren Gruppen gemäß dem eingegebenen String. Verwenden Sie dieses Feld, um die Liste der verfügbaren Gruppen auszuarbeiten.

Verfügbare Benutzer. Listet die erkannten Benutzer auf, die der Gruppe hinzugefügt werden können.

Gruppe enthält Benutzer. Listet die Benutzer auf, die der Gruppe zugewiesen sind.

Alle hinzufügen. Assoziiert alle Benutzer mit der Gruppe.

Alle entfernen. Entfernt alle angezeigten Benutzer aus der Gruppe.

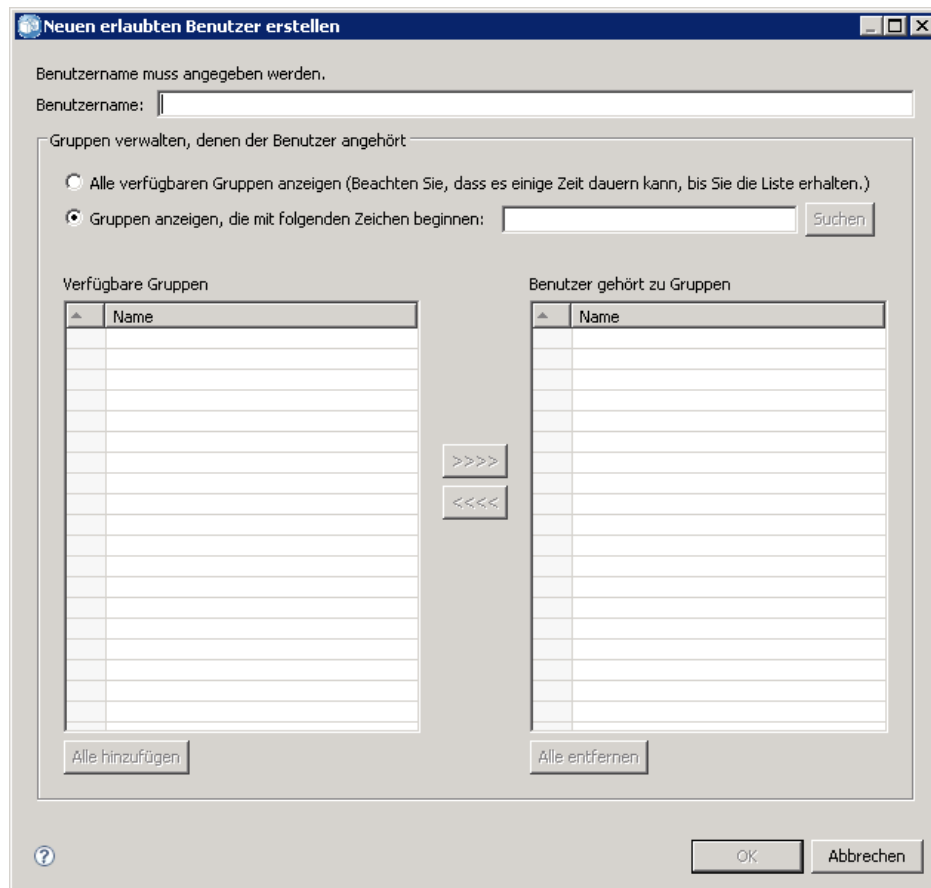
Für das Erstellen einer erweiterten Gruppe muss der Benutzername angegeben werden. Der Gruppe können auch Benutzer hinzugefügt werden.

1. Geben Sie den Gruppennamen an.
2. Fügen Sie der Gruppe bei Bedarf Benutzer hinzu.
3. Klicken Sie auf OK. Die neue erweiterte Gruppe erscheint in der Liste im Editor "Benutzer und Gruppen verwalten".

Erstellen eines erlaubten Benutzers

Klicken Sie im Editor "Benutzer und Gruppen verwalten" für "Active Directory mit lokalem Überschreiben" auf Neuer erlaubter Benutzer. Das Dialogfeld "Neuen erlaubten Benutzer erstellen" wird geöffnet.

Abbildung 4-10
Dialogfeld "Neuen erlaubten Benutzer erstellen"



Benutzername. Der Name unterscheidet keine Groß-/Kleinschreibung und kann Leerzeichen enthalten. Beachten Sie, dass es nicht möglich ist, zu prüfen, ob der Benutzer tatsächlich im Remote-Verzeichnis existiert. Ein falsch eingegebener Benutzername wird nie beim System authentifiziert.

Alle erweiterten Gruppen anzeigen. Liefert eine Liste aller erweiterten Gruppen.

Gruppen anzeigen, die mit folgenden Zeichen beginnen. Filtert die Liste mit den verfügbaren Gruppen gemäß dem eingegebenen String. Verwenden Sie dieses Feld, um die Liste der verfügbaren Gruppen auszuarbeiten.

Verfügbare Gruppen. Listet die erkannten Gruppen auf, denen der Benutzer zugewiesen werden kann.

Benutzer gehört zu Gruppen. Listet die Gruppen auf, denen der Benutzer derzeit zugewiesen ist.

Alle hinzufügen. Assoziiert alle Gruppen mit dem Benutzer.

Alle entfernen. Entfernt alle angezeigten Gruppen vom Benutzer.

Anmerkung: Ein erlaubter Benutzer kann nur dann mit erweiterten Gruppen assoziiert werden, wenn die erweiterten Gruppen für "Active Directory mit lokalem Überschreiben" aktiviert sind. Wenn erweiterte Gruppen nicht aktiviert sind, werden die Felder zur Benutzerauswahl nicht angezeigt.

Für das Erstellen eines erlaubten Benutzers muss der Benutzername angegeben werden. Der Benutzer kann außerdem mit Gruppen assoziiert werden.

1. Geben Sie im Dialogfeld "Neuen Benutzer erstellen" den Benutzernamen ein.
2. Assoziieren Sie den Benutzer bei Bedarf mit erweiterten Gruppen.
3. Klicken Sie auf OK. Der neue erlaubte Benutzer erscheint in der Liste im Editor "Benutzer und Gruppen verwalten".

Rollen

Überblick über Rollen

Rollen ermöglichen die Verwaltung des Zugriffs von Benutzern und Gruppen auf die Systemfunktionen. Rollen werden Benutzern und Gruppen zugewiesen und werden zusammen mit einem Security-Provider eingesetzt.

Mit jeder erstellten Rolle sind Aktionen verbunden, die den Berechtigungen und dem Maß an Kontrolle entsprechen, über die der Benutzer oder die Gruppe verfügt, der/die der Rolle zugeordnet wird. Zum Beispiel kann eine grundlegende Benutzerrolle erstellt werden. Der grundlegenden Benutzerrolle wird ein beschränktes Set von Aktionen für den Zugriff auf das System und das Anzeigen von Inhalten des Repository zugeordnet. In der grundlegenden Benutzerrolle sind die Aktionen zur Definition von Servern, zum Hinzufügen anderer Benutzer oder zur Definition von Systemkonfigurationen, die sich auf andere Benutzer und Gruppen auswirken würden, nicht enthalten.

Zur Ausführung von administrativen Aufgaben, z. B. Löschen von Benutzern, Erstellen von Gruppen und Definieren zusätzlicher Rollen, wird jedoch eine erweiterte Benutzerrolle benötigt. In diesem Fall kann eine weniger beschränkte Rolle erstellt werden, die mehr Kontrolle über die Anwendungsdomäne ermöglicht und einer sehr kleinen Reihe von Benutzern zugewiesen wird.

Die Liste verfügbarer Aktionen ist innerhalb des Systems definiert und kann von dem Benutzer, der die Aktionen zuordnet, nicht bearbeitet werden.

Falls der Benutzer mehreren Gruppen angehört, enthalten die diesem Benutzer zugewiesenen Rollen – ein Aktions-Set – alle Rollen, die dem Benutzer explizit zugeordnet werden, sowie alle Rollen, die ihm im Zuge der Gruppenzugehörigkeit indirekt zugeordnet werden. Falls dem Benutzer oder der Gruppe verschiedene Rollen zugeordnet werden, besteht das Aktions-Set des Benutzers oder der Gruppe aus allen explizit zugeordneten Rollen sowie den Rollen, die ihm/ihr im Zuge der Gruppenzugehörigkeit zugeordnet wurden. Benutzer und Gruppen müssen nach Sicherheits-Provider verwaltet werden; Rollen werden Provider-übergreifend verwaltet. Weitere Informationen zu der Verwaltung von Benutzern und Gruppen finden Sie unter [Kapitel 4](#).

Mithilfe des Tools Server-Administration von IBM® SPSS® Collaboration and Deployment Services Deployment Manager können Sie Rollendefinitionen verwalten und die Benutzer und Gruppen ändern, die den Rollen zugewiesen sind.

Aktionen

Eine Rolle besteht aus einer Liste von Aktionen. Diese Aktionen sind durch das System definiert und können nicht geändert werden.

IBM SPSS Collaboration and Deployment Services Aktionen

- **Zugriff auf Inhalte und Ordner.** Zugriff auf das IBM® SPSS® Collaboration and Deployment Services Repository.
- **Zugriff auf gesammelte Feeds.** Zugriff auf gesammelte Feeds, z. B. RSS-(Really Simple Syndication-)Feeds.
- **Konfiguration.** Bearbeiten der Repository-Einstellungen.
- **Modell konfigurieren.** Modelle für Scoring konfigurieren.
- **Erstellen von Abonnements.** Erstellen von individuellen Abonnements für Repository-Objekte wie Ordner, Dateien, Jobs usw. Die Abonnenten erhalten E-Mail-Benachrichtigungen, sobald an den entsprechenden Objekten Änderungen vorgenommen werden.
- **Benachrichtigungen definieren und verwalten.** Definieren und Verwalten von Benachrichtigungen für mehrere Personen im Fall von Ereignissen wie erfolgreichen oder fehlgeschlagenen Jobs.
- **Anmeldeinformationen definieren.** Sichere Anmeldeinformationen für Ausführungsserver erstellen, anzeigen und ändern.
- **Benutzerdefinierte Eigenschaften definieren.** Definieren und Bearbeiten von benutzerdefinierten Eigenschaften für Objekte innerhalb des Repository.
- **Datenquellen definieren.** Definieren und Bearbeiten von Datenquellen.
- **Meldungsdomänen definieren.** Definieren und Bearbeiten von Domänen für JMS-Meldungen.
- **Definieren von Server-Clustern.** Ausführungsserver-Cluster definieren und bearbeiten.
- **Server definieren.** Ausführungsserver definieren und bearbeiten.
- **Themen definieren.** Definieren und Bearbeiten der Themen-Hierarchie für das Repository.
- **Job Edit.** Erstellen und Bearbeiten von Jobs. Beachten Sie, dass die Sichtbarkeit von Jobs für Benutzer von deren Berechtigungen abhängt.
- **Jobausführung.** Jobs ausführen. Beachten Sie, dass die Sichtbarkeit von Jobs für Benutzer von deren Berechtigungen abhängt.
- **Sperren verwalten** Verwalten von Sperren, die Benutzer für Repository-Ressourcen erstellen; z. B. Freischalten von Ressourcen, die von anderen Benutzern gesperrt wurden.
- **IBM® SPSS® Collaboration and Deployment Services Enterprise View verwalten.** Enterprise-Ansichten, Anwendungsansichten und Daten-Provider-Definitionen erstellen, bearbeiten und löschen.
- **Abonnements verwalten.** Verwalten und Löschen der Abonnements anderer Benutzer.
- **MIME-Typen.** Verwalten von MIME-Typzuordnungen für das Repository.
- **Repository-Index.** Erstellen eines neuen Index für den Inhalt des Repository.
- **Benutzerdefinierte Dialogfelder ausführen** Benutzerdefinierte IBM® SPSS® Statistics-Dialogfelder ausführen.
- **Bericht dynamisch ausführen.** Ausführen von dynamischen Berichten, wie z. B. Business Intelligence Reporting Tools-Berichte (BIRT), in IBM® SPSS® Collaboration and Deployment Services Deployment Portal.
- **Zeitpläne.** Verwalten von Job-Zeitplänen.

- **Modell scoren.** Modelle scoren.
- **Alle Versionen anzeigen.** Anzeigen aller Versionen von (bezeichneten und unbezeichneten) Objekten in Deployment Portal. Standardmäßig sind Benutzer lediglich zur Anzeige bezeichneter Versionen in Deployment Portal berechtigt.
- **Letzte anzeigen.** Nur die aktuellste Objektversion anzeigen.
- **Arbeit übergeben** Übergeben von Arbeit (z. B. von Berichten) zur Verarbeitung durch IBM® SPSS® Collaboration and Deployment Services.
- **Verwaltung der Benutzervoreinstellungen.** Verwalten der Voreinstellungen anderer Benutzer.
- **Abgelaufene Dateien anzeigen.** Anzeigen von abgelaufenen Inhalten, wie z. B. Dateien und Jobs.
- **Model Management Dashboard anzeigen.** Anzeigen von Model Management Dashboards in IBM® SPSS® Collaboration and Deployment Services Deployment Manager und Deployment Portal.

Anmerkung: Die Aktion *Letzte anzeigen* ist eine Untergruppe von *Alle Versionen anzeigen* und wenn ein Benutzer beide Aktionen ausführt, hat *Alle Versionen anzeigen* Vorrang vor *Letzte anzeigen*.

Administrator-Rolle

Das System umfasst eine vordefinierte Rolle für *Administratoren*, die nicht geändert werden kann. Diese Rolle ist mit allen im System verfügbaren Aktionen verknüpft. Jeder Benutzer mit dieser Rolle kann jede beliebige Aktion im System ausführen. Zudem steht einige Funktionalität, die nicht durch Aktionen gesteuert wird, z. B. Export und Import von Repository-Inhalten, nur Benutzern mit dieser Rolle zur Verfügung.

Aufgrund der weitreichenden Steuerungsmöglichkeiten für Administratoren sollte man beim Zuweisen von Benutzern zu dieser Rolle besondere Sorgfalt walten lassen. Weisen Sie nur die Benutzer zu, die Zugriff auf sämtliche Funktionalität im System benötigen. Benutzer, die nur eine Untergruppe an Aktionen benötigen, sollten benutzerdefinierten Rollen zugewiesen werden. Für weitere Informationen siehe Thema [Erstellen einer neuen Rolle](#) auf S. 43.

Rollendefinitionen verwalten

Wenn Sie mit Rollen arbeiten möchten, wählen Sie Server-Administration aus dem Menü “Extras”, wählen einen IBM® SPSS® Collaboration and Deployment Services Repository-Server aus und melden sich an. Doppelklicken Sie dann auf das Symbol Rollen, damit der Server auf den Editor “Rollendefinitionen verwalten” zugreift.

Abbildung 5-1
Verwalten von Rollendefinitionen sowie Benutzer- und Gruppenzuordnungen

Rollendefinitionen sowie Benutzer- und Gruppenzuweisungen verwalten

Alle Rollen		Definitionen der Rolle:		Der Rolle zugewiesene Benutzer und Gruppen:	
Rollen		Aktionen		Mitglieder	
Administratoren					

Beachten Sie, dass alle Änderungen in diesem Editor sofort wirksam werden und es nicht möglich ist, Änderungen zu widerrufen.

Alle Rollen. Zeigt eine Liste aller Rollen, die für den Sicherheits-Provider verfügbar sind. Wenn neue Rollen hinzugefügt werden, wird diese Liste mit Einträgen gefüllt. Um dem System eine neue Rolle hinzuzufügen, klicken Sie auf die Schaltfläche Neue Rolle. Um eine Rolle zu löschen, wählen Sie die Rolle aus und klicken Sie auf die Schaltfläche Löschen. Wählen Sie eine Rolle aus dieser Liste, um ihre assoziierten Aktionen zu sehen.

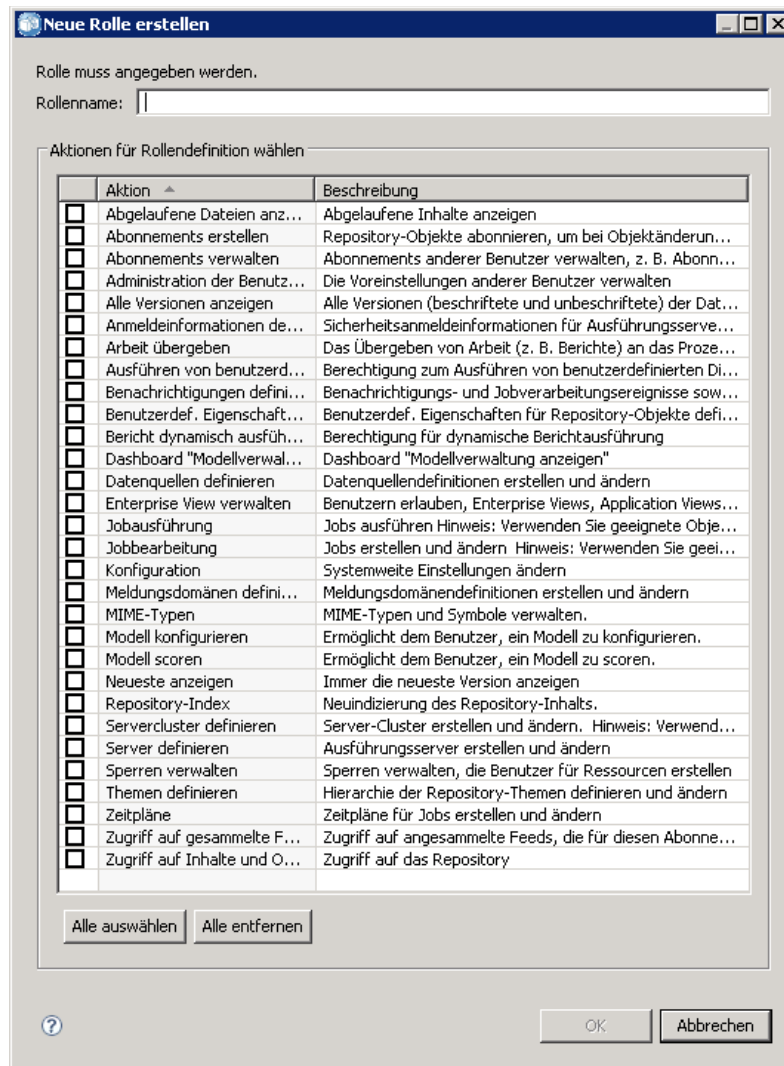
Definition von Rollen. Zeigt eine Liste der Aktionen, die mit einer ausgewählten Rolle assoziiert sind. Um die Aktionen zu bearbeiten, die mit einer ausgewählten Rolle verknüpft sind, klicken Sie auf die Schaltfläche Aktionen bearbeiten.

Der Rolle zugewiesene Benutzer und Gruppen. Eine Liste der Benutzer und Gruppen, die einer ausgewählten Rolle zugewiesen sind. Um die Benutzer- und Gruppenliste für eine ausgewählte Rolle zu bearbeiten, klicken Sie auf die Schaltfläche Benutzer und Gruppen bearbeiten.

Erstellen einer neuen Rolle

Um eine neue Rolle zu erstellen, klicken Sie im Rolleneditor auf die Schaltfläche Neue Rolle. Das Dialogfeld "Neue Rolle erstellen" wird geöffnet.

Abbildung 5-2
Dialogfeld "Neue Rolle erstellen"



Rollenname. Ein Textstring zur Identifizierung der Rolle. Der Rollenname muss eindeutig sein und darf keinen anderen Rollennamen duplizieren.

Aktion. Enthält alle Aktionen, die im System definiert und verfügbar sind. Anfangs sind mit einer Rolle keine Aktionen assoziiert.

Markieren Sie das Kästchen neben einer Aktion, um die Aktion der Rolle zuzuweisen. Klicken Sie alternativ auf die Schaltfläche **Alle auswählen**, um der Rolle alle Aktionen hinzuzufügen. Durch Klicken auf die Schaltfläche **Alle entfernen** werden alle Aktionen von der Rolle entfernt. Die Aktionenliste kann durch Klicken auf die Spalte **Aktion** sortiert werden. Klicken Sie auf **OK**, um die Rolle zu erstellen und zu speichern.

Bearbeiten einer Rolle

Wenn Sie die Liste der Aktionen bearbeiten möchten, die einer Rolle zugewiesen sind, wählen Sie die Rolle im Rolleneditor aus und klicken auf die Schaltfläche Aktionen bearbeiten. Das Dialogfeld "Rolle bearbeiten" wird geöffnet.

Rollename. Ein Textstring zur Identifizierung der Rolle. Der Rollename muss eindeutig sein und darf keinen anderen Rollennamen duplizieren.

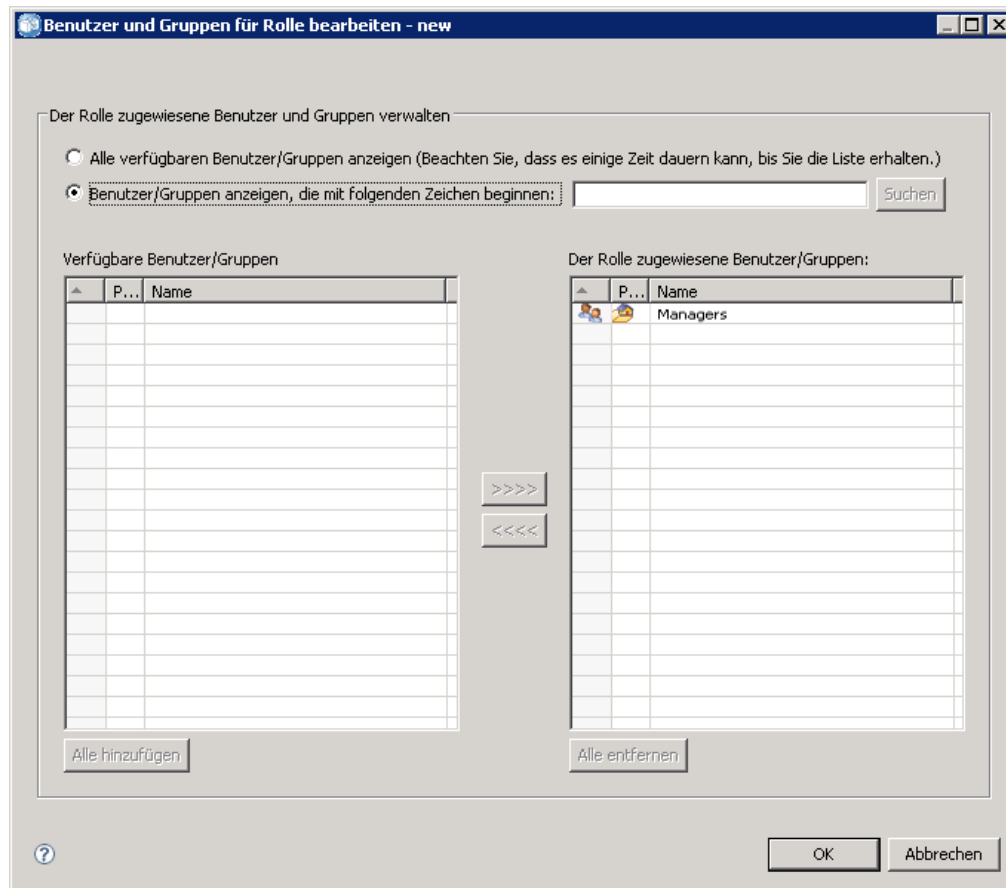
Aktion. Enthält alle Aktionen, die im System definiert und verfügbar sind. Anfangs sind mit einer Rolle keine Aktionen assoziiert.

Markieren Sie das Kästchen neben einer Aktion, um die Aktion der Rolle zuzuweisen. Klicken Sie alternativ auf die Schaltfläche Alle auswählen, um der Rolle alle Aktionen hinzuzufügen. Durch Klicken auf die Schaltfläche Alle entfernen werden alle Aktionen von der Rolle entfernt. Die Aktionenliste kann durch Klicken auf die Spalte Aktion sortiert werden. Klicken Sie auf OK, um die geänderte Rollendefinition zu speichern.

Bearbeiten von Benutzern und Gruppen, die einer Rolle zugewiesen sind

Sobald Rollen definiert sind, müssen sie mit Benutzern und Gruppen assoziiert werden, um Zugriffsebenen zu definieren. Um einer Rolle Benutzer und Gruppen zuzuweisen, klicken Sie im Rolleneditor auf die Schaltfläche Benutzer und Gruppen bearbeiten. Das Dialogfeld "Benutzer und Gruppen für Rolle bearbeiten" wird geöffnet.

Abbildung 5-3
Dialogfeld "Benutzer und Gruppen für Rolle bearbeiten"



Für die Anzeige von Benutzern und Gruppen, die sich Rollen zuweisen lassen, gibt es zwei Optionen:

- **Alle verfügbaren Benutzer/Gruppen anzeigen.** Zeigt eine Liste aller Benutzer und Gruppen, die für alle Sicherheits-Provider verfügbar sind.
- **Benutzer/Gruppen anzeigen, die mit folgenden Zeichen beginnen.** Filtert die Liste mit den verfügbaren Benutzern und Gruppen gemäß den Suchoptionen.

Die Liste "Verfügbare Benutzer/Gruppen" wird gemäß den Suchoption mit Benutzern und Gruppen gefüllt. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf die Schaltfläche >>>>, um ihn bzw. sie der Rolle zuzuweisen. Wenn Sie einen Benutzer oder eine Gruppe von einer Rolle entfernen möchten, wählen Sie den Benutzer bzw. die Gruppe in der Liste "Der Rolle zugewiesene Benutzer/Gruppen" aus und klicken auf die Schaltfläche <<<<. Klicken Sie zum Abschluss auf OK.

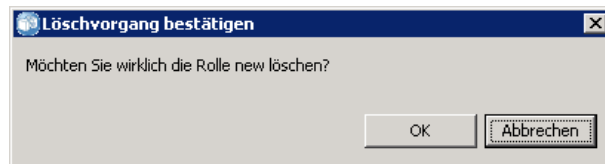
Entfernen einer Rolle

So entfernen Sie eine Rolle:

1. Wählen Sie im Rolleneditor die Rolle aus, die Sie entfernen möchten.
2. Klicken Sie auf die Schaltfläche Löschen. Es wird ein Bestätigungs-Dialogfeld geöffnet.

Abbildung 5-4

Dialogfeld "Löschvorgang bestätigen"



3. Klicken Sie auf OK, um zu bestätigen, dass die Rolle entfernt werden soll.

Die Rolle wird aus dem System entfernt.

Sicherheits-Provider

Ein Sicherheits-Provider gleicht die Anmeldeinformationen, die ein Benutzer angibt, mit einem bestimmten Benutzerverzeichnis ab. IBM® SPSS® Collaboration and Deployment Services verfügt über ein internes Verzeichnis für die Authentifizierung, es kann jedoch auch ein vorhandenes Benutzerverzeichnis des Unternehmens verwendet werden. Zu den verfügbaren Providern gehören:

- **Nativ (oder lokales Benutzer-Repository).** Der interne Sicherheits-Provider für IBM SPSS Collaboration and Deployment Services, in dem Benutzer, Gruppen und Rollen definiert werden können. Der native Provider ist immer aktiv und kann nicht deaktiviert werden.
- **Active Directory®.** Die Microsoft-Version des Lightweight Directory Access Protocol (LDAP) für Authentifizierung, Autorisierung und Sicherheitsrichtlinien. Benutzer und Gruppen für diesen Provider müssen direkt im Active Directory-Framework definiert werden. Nachdem Active Directory für die Verwendung mit IBM SPSS Collaboration and Deployment Services konfiguriert wurde, kann das System einen Benutzer über den Active Directory-Server authentifizieren, wobei die Berechtigungen und Zugriffsrechte für diesen Benutzer beibehalten werden. Im Gegensatz zum nativen Provider kann dieser Provider aktiviert und deaktiviert werden. Weitere Informationen zu Active Directory finden Sie in der Original-Herstellerdokumentation.
- **Active Directory mit lokaler Überschreibung.** Ein Provider, der Active Directory verwendet, aber die Erstellung erweiterter Gruppen und Filter für erlaubte Benutzer ermöglicht. Eine erweiterte Gruppe enthält eine Liste von Benutzern aus Active Directory, existiert jedoch außerhalb des Active Directory-Framework. Ein Filter für erlaubte Benutzer beschränkt die Liste von Active Directory-Benutzern, die vom System authentifiziert werden können, auf ein definiertes Set von Benutzern. Dieser Provider kann aktiviert oder deaktiviert werden.
- **IBM i.** Das IBM i-Benutzerprofileverzeichnis kann verwendet werden, um IBM SPSS Collaboration and Deployment Services-Benutzer zu authentifizieren. Dieser Provider kann aktiviert oder deaktiviert werden. Wenn der IBM i-Sicherheits-Provider mit einer IBM SPSS Collaboration and Deployment Services-Installation mit aktivierter Einzelanmeldung verwendet wird, muss EIM (Enterprise Identity Management) aktiviert sein. Zusätzlich muss */QIBM/UserData/Java400/ext/eim.jar* in das Bibliotheksverzeichnis des IBM SPSS Collaboration and Deployment Services-Anwendungsservers kopiert werden, wenn der Anwendungsserver auf einem Nicht-IBM i-Host läuft.
- **JDE-Anwendungsbenutzer.** Wenn Sie IBM® ShowCase® verwenden, wird dieser Sicherheits-Provider bei der Installation des IBM ShowCase-Adapters in Ihrem IBM SPSS Collaboration and Deployment Services-Server installiert. Dieser Sicherheits-Provider kann so konfiguriert werden, dass sich JD Edwards-(JDE-)Anwendungsbenutzer anmelden und die IBM SPSS Collaboration and Deployment Services-Umgebung verwenden können. Anleitungen finden Sie im *IBM ShowCase-Administratorhandbuch*.

- **OpenLDAP®.** Eine Open-Source-LDAP-Implementierung für Authentifizierung, Autorisierung und Sicherheitsrichtlinien. Benutzer und Gruppen für diesen Provider müssen direkt unter Verwendung der LDAP-Tools definiert werden. Nachdem OpenLDAP für die Verwendung mit IBM SPSS Collaboration and Deployment Services konfiguriert wurde, kann das System einen Benutzer über den OpenLDAP-Server authentifizieren, wobei die Berechtigungen und Zugriffsrechte für diesen Benutzer beibehalten werden. Dieser Provider kann aktiviert oder deaktiviert werden.
- **SiteMinder®.** Computer Associates Zugriff-Management-System für Web-Anwendungen von Unternehmen für richtlinienbasierte Authentifizierung und Autorisierung. Benutzer und Gruppen für diesen Provider werden in einem externen LDAP-basierten Verzeichnis festgelegt, während Zugriffsrichtlinien in SiteMinder festgelegt werden. Der Provider ermöglicht außerdem das Erstellen von erweiterten Gruppen und die Filterung nach berechtigten Benutzern.

Wichtig: Der SiteMinder-Sicherheits-Provider ist standardmäßig nicht aktiviert. Um die SiteMinder-Authentifizierung zu aktivieren, muss *siteminder.package* aus dem Ordner *optional* auf dem IBM SPSS Collaboration and Deployment Services-Installationsdatenträger installiert werden.

Sicherheits-Provider in IBM SPSS Collaboration and Deployment Services Deployment Manager

Bevor Sie Aktionen mit Sicherheits-Providern ausführen, navigieren Sie zur administrativen Schnittstelle, die diese Funktionalität steuert.

1. Wählen Sie im Menü “Extras” die Option Server-Verwaltung.
2. Melden Sie sich in der Registerkarte “Server-Administration” bei einem IBM® SPSS® Collaboration and Deployment Services-Server an.
3. Doppelklicken Sie auf das Symbol Konfiguration für den Server, um die Hierarchie zu erweitern.
4. Doppelklicken Sie auf das Symbol Sicherheitsanbieter, um die Hierarchie zu erweitern.
5. Doppelklicken Sie auf den Sicherheits-Provider, den Sie konfigurieren möchten.

Abbildung 6-1
Zugreifen auf Sicherheits-Provider



Konfigurieren von Sicherheits-Providern

Jeder Sicherheits-Providertyp verfügt über Einstellungen, die für die Art des eingesetzten Authentifizierungs- und Autorisierungssystems typisch sind.

Native

Der Native-Sicherheits-Provider ist IBM® SPSS® Collaboration and Deployment Services-intern und umfasst keine Einstellungen, die konfiguriert werden können.

Active Directory

Zum Konfigurieren der Active Directory-Einstellungen doppelklicken Sie auf das Symbol Active Directory.

Abbildung 6-2
Active Directory-Konfiguration

The screenshot shows a configuration window titled "Sicherheits-Provider-Konfiguration" for Active Directory. The window includes the following elements:

- Aktivieren
- Host-URL: ldap://hostname
- Benutzer-Basis-DN: OU=USERS,OU=MYUNIT,DC=company,DC=com
- Gruppen-Basis-DN: OU=GROUPS,OU=MYUNIT,DC=company,DC=com
- Domäne: MYDOMAIN
- Domänenbenutzer: domain\userID
- Passwort des Domänenbenutzers: (two masked password fields)
- SSL verwenden

- **Aktivieren.** Aktiviert und deaktiviert die Verwendung von **Active Directory** als Service-Provider.
- **Host-URL.** URL für den Active Directory-Server. Der Standardport für LDAP ist 389.
- **Benutzer-Basis-DN.** Basis-Distinguished-Name für Benutzersuchen.
- **Gruppen-Basis-DN.** Basis-Distinguished-Name für Gruppensuchen.
- **Domäne.** Der DNS-Namespace, in dem sich der Benutzer anmeldet.
- **Domänenbenutzer.** Eine Benutzer-ID, um Suchen im Format *Domäne\Benutzername* durchzuführen. Der angegebene Name muss über die entsprechenden Berechtigungen verfügen, um nach Benutzern zu suchen und diese zu authentifizieren.
- **Passwort des Domänenbenutzers.** Aus Sicherheitsgründen wird das Passwort des Domänenbenutzers durch Sternchen (*) ersetzt. Geben Sie den Wert in beide Passwortfelder ein, um den korrekten Wert zu bestätigen.
- **SSL verwenden.** Wählen Sie die Verwendung von Secure Sockets für die Kommunikation mit dem Active Directory-Server.

Wenn Sie die gewünschten Einstellungen vorgenommen haben, wählen Sie Speichern aus dem Menü "Datei".

Active Directory mit lokaler Überschreibung

Um die Einstellungen für Active Directory mit lokalem Überschreiben zu konfigurieren, doppelklicken Sie auf das Symbol Active Directory mit lokalem Überschreiben. Die meisten Einstellungen sind identisch mit denen für Active Directory. Jedoch bietet das lokale Überschreiben zwei zusätzliche Einstellungen.

Abbildung 6-3
Konfiguration von Active Directory mit lokalem Überschreiben

The screenshot shows a Windows dialog box titled "Sicherheits-Provider-Konfiguration" for "Active Directory mit lokalem Überschreiben auf Admin". The dialog contains the following fields and options:

- Aktivieren
- Host-URL: ldap://hostname
- Benutzer-Basis-DN: OU=USERS,OU=MYUNIT, DC=company,DC=com
- Gruppen-Basis-DN: OU=GROUPS,OU=MYUNIT, DC=company,DC=com
- Domäne: MYDOMAIN
- Domänenbenutzer: domain\userID
- Passwort des Domänenbenutzers: (two masked password fields)
- SSL verwenden
- Erlaubte Benutzer
- Erweiterte Gruppen

- **Erlaubte Benutzer.** Aktiviert oder deaktiviert die Verwendung erlaubter Benutzer, wodurch nur Benutzer in einer lokal definierten Liste in Active Directory authentifiziert werden können.
- **Erweiterte Gruppen.** Aktiviert und deaktiviert die Verwendung erweiterter Gruppen, wodurch eine Gruppe von Active Directory-Benutzern definiert werden kann. Active Directory-Benutzer können diesen lokalen Gruppen zugewiesen werden.

Wenn Sie die gewünschten Einstellungen vorgenommen haben, wählen Sie Speichern aus dem Menü "Datei".

OpenLDAP

Zum Konfigurieren der OpenLDAP-Einstellungen doppelklicken Sie auf das Symbol OpenLDAP.

Abbildung 6-4
OpenLDAP-Konfiguration

OpenLDAP auf Admin

Sicherheits-Provider-Konfiguration

Aktivieren

Host-URL:

Benutzer-Basis-DN:

Gruppen-Basis-DN:

SearchUser:

SearchUser-Passwort:

SSL verwenden

- **Aktivieren.** Aktiviert und deaktiviert die Verwendung von OpenLDAP als Sicherheits-Provider.
- **Host-URL.** Der Pfad zum LDAP-Server, in der Regel ein DNS-auflösbarer Name oder eine IP-Adresse (beispielsweise *ldap://*). Der Standardport für LDAP ist 389.
- **Benutzer-Basis-DN.** Basis-Distinguished-Name für Benutzersuchen.
- **Gruppen-Basis-DN.** Basis-Distinguished-Name für Gruppensuchen.
- **SearchUser.** Eine Benutzer-ID, um Suchen in einem Distinguished-Name-Format durchzuführen. Der angegebene Name muss über die entsprechenden Berechtigungen verfügen, um nach Benutzern zu suchen und diese zu authentifizieren.
- **SearchUser-Passwort.** Aus Sicherheitsgründen wird das Passwort des Domänenbenutzers durch Sternchen (*) ersetzt. Geben Sie den Wert in beide Passwortfelder ein, um den korrekten Wert zu bestätigen.

Wenn Sie die gewünschten Einstellungen vorgenommen haben, wählen Sie Speichern aus dem Menü "Datei".

IBM i

Doppelklicken Sie zum Konfigurieren des IBM i-Sicherheits-Providers auf das Symbol IBM i.

Abbildung 6-5
IBM i-Konfiguration

- **Aktivieren.** Aktiviert und deaktiviert die Verwendung eines IBM i-Systems als Sicherheits-Provider.
- **IBM i Server.** Der Pfad zum IBM i-System, in der Regel ein DNS-auflösbarer Name oder eine IP-Adresse. Wenn Sie IBM i-Sicherheits-Provider mit Enterprise Identity Management (EIM) verwenden, um die Einzelanmeldung für IBM® SPSS® Collaboration and Deployment Services zu aktivieren, muss dieser Wert mit dem EIM-Zielregistrierungswert übereinstimmen. Wenn der EIM-Zielregistrierungswert ein vollständig qualifizierter Name des Hosts ist, geben Sie den vollständig qualifizierten Hostnamen ein.
- **Benutzerprofil.** Das Benutzerprofil, das für Verzeichnissuchen im IBM i-System verwendet wird.
- **Paßwort.** Das Passwort für das angegebene IBM i-Profil. Aus Sicherheitsgründen wird das Passwort des Domänenbenutzers durch Sternchen (*) ersetzt. Geben Sie den Wert in beide Passwortfelder ein, um den korrekten Wert zu bestätigen.
- **EIM-Suche aktivieren.** Für IBM SPSS Collaboration and Deployment Services-Installationen mit aktivierter Einzelanmeldung wird angezeigt, dass Enterprise Identity Management aktiviert ist.
- **EIM-Server.** Enterprise Identity Management-Host-URL.
- **EIM-Benutzer.** Der Benutzername für die Enterprise Identity Management-Host-Anmeldung.
- **EIM-Passwort.** Das Passwort für den angegebenen Enterprise Identity Management-Benutzer.

Anmerkung: Jedes IBM i-Benutzerprofil kann für Verzeichnissuchen verwendet werden, aber die Liste der Profile, die zurückgegeben wird, ist nach der Berechtigung des Profils gefiltert, das für die Suche verwendet wird. Wenn Sie einen Benutzer auf QSECOFR-Ebene angeben, werden alle Profile im System zurückgegeben. Wenn Sie einen Benutzer mit weniger Berechtigungen

verwenden, werden basierend auf den Sicherheitseinstellungen der Benutzerprofile weniger Profile zurückgegeben.

IBM i-Benutzer- und -Gruppenberechtigungen

Wenn ein IBM i-Benutzerprofil als Gruppe verwendet werden soll, müssen dem Profil andere IBM i-Profilen zugeordnet werden, bevor ihm IBM SPSS Collaboration and Deployment Services-Berechtigungen zugeordnet werden. Andernfalls werden die Berechtigungen nicht an andere IBM i-Benutzer weitergegeben. Wenn beispielsweise ein IBM i-Benutzer *test* erstellt wird, ihm in IBM SPSS Collaboration and Deployment Services Berechtigungen zugewiesen werden und er dann als Gruppe einem IBM i-Benutzer *test2* zugeordnet wird, erhält *test2* nicht die Berechtigungen von *test* in IBM SPSS Collaboration and Deployment Services. Wenn *test2* hingegen *test* zugeordnet wird, bevor die IBM SPSS Collaboration and Deployment Services-Berechtigungen von *test* definiert werden, übernimmt *test2* die Berechtigungen.

Benutzer von IBM ShowCase und JD Edwards (JDE)

Wenn Sie IBM® ShowCase® verwenden, informieren Sie sich in der zusammen mit diesem Produkt installierten Dokumentation in Bezug auf Sicherheits-Provider und Integration mit IBM SPSS Collaboration and Deployment Services.

JDE-Anwendungsbenuer

Nach der Installation von IBM® SPSS® Collaboration and Deployment Services – Server-Adapter für ShowCase ermöglicht der Sicherheits-Provider für JDE-Anwendungsbenuer den Endbenutzern von Deployment Manager und Deployment Portal die Anmeldung als Oracle JDE-Anwendungsbenuer. Anleitungen finden Sie im *IBM® ShowCase®-Administratorhandbuch*.

SiteMinder-Sicherheits-Provider

Doppelklicken Sie zum Konfigurieren der SiteMinder-Einstellungen auf das Symbol SiteMinder.

Abbildung 6-6
SiteMinder-Konfiguration

Parameter	Value
<input type="checkbox"/> Aktivieren	
Local Computer	127.0.0.1
Site Minder IP	127.0.0.1
Agent Secret

Directory Root	OU=NEWYORK, DC=spss, DC=COM
Organization Root	OU=USERS, OU=NEWYORK, DC=spss, DC=COM
Directory Server IP	127.0.0.1
Directory User Name	SiteMinder
Directory User Password

Directory Name	SPSS AD
Directory Search User Query	(&(objectCategory=user)(sAMAccountName=\$ID))
Directory Search Group Query	(&(objectCategory=group)(sAMAccountName=\$ID))

- **Aktivieren.** Aktiviert und deaktiviert die Verwendung von SiteMinder als Sicherheits-Provider.
- **Lokaler Computer.** IBM® SPSS® Collaboration and Deployment Services-Host-Adresse oder -Domänenname.
- **SiteMinder IP.** Server-Adresse oder Domänenname der SiteMinder-Richtlinie.
- **Agentengeheimnis.** Agentengeheimnis für den Agenten *spss-agent*; wird für die Anmeldung an den SiteMinder-Richtlinien-Server verwendet.
- **Stammverzeichnis.** Stammverzeichnis-Basis-DN, zum Beispiel DC=Domänenname Teil 1, DC=Domänenname Teil 2
- **Organisationsstamm.** Organisationsstamm, zum Beispiel OU=Einheit, DC=Domänenname Teil 1, DC=Domänenname Teil 2 ...
- **Verzeichnisserver.** Verzeichnis der Server-Adresse oder Domänenname.
- **Verzeichnis-Benutzername.** Der Name des Benutzers für die Verzeichnisanmeldung.
- **Verzeichnis-Benutzerpasswort.** Das Passwort für die Verzeichnisanmeldung.
- **Verzeichnisname.** LDAP-Verzeichnisname.
- **Benutzerabfrage für Verzeichnissuche.** LDAP-Abfrage für benutzerbasierte Authentifizierung.
- **Gruppenabfrage für Verzeichnissuche.** LDAP-Abfrage für gruppenbasierte Authentifizierung.

Wenn Sie die gewünschten Einstellungen vorgenommen haben, wählen Sie Speichern aus dem Menü "Datei".

Sicherheits-Provider im browserbasierten IBM SPSS Collaboration and Deployment Services Deployment Manager

So aktivieren Sie die Seite “Sicherheits-Provider”:

- ▶ Klicken Sie in der Navigationsliste auf Sicherheits-Provider. Die Seite “Sicherheits-Provider” wird angezeigt.

Abbildung 6-7
Seite “Sicherheits-Provider”



So ändern Sie die verwendeten Sicherheits-Provider:

- ▶ Aktivieren oder deaktivieren Sie die Kontrollkästchen neben dem Sicherheits-Provider.
- ▶ Klicken Sie auf Setzen.

Konfigurieren von Sicherheits-Providern

Jeder Sicherheits-Providertyp verfügt über Einstellungen, die für die Art des eingesetzten Authentifizierungs- und Autorisierungssystems typisch sind.

Nativ

Der native (bzw. lokale) Sicherheits-Provider ist systeminhärent und kann nicht entfernt werden. Dem nativen Sicherheitssystem können Benutzer hinzugefügt werden, das System kann jedoch weder deaktiviert noch konfiguriert werden.

Active Directory

Um die Active Directory-Einstellungen zu konfigurieren, klicken Sie rechts neben dem Kontrollkästchen “Active Directory über LDAP” auf Einstellungen bearbeiten. Die aktuellen Einstellungen werden angezeigt. Folgende Einstellungen können geändert werden:

- **Host-URL.** URL für den **Active Directory**-Server. Der Standardport für LDAP ist 389.
- **Benutzer-Basis-DN.** Basis-**Distinguished-Name** für Benutzersuchen.

- **Gruppen-Basis-DN.** Basis-Distinguished-Name für Gruppensuchen.
- **Domäne.** Der DNS-Namespace, in dem sich der Benutzer anmeldet.
- **Domänenbenutzer.** Eine Benutzer-ID, um Suchen im Format *Domäne\Benutzername* durchzuführen. Der angegebene Name muss über die entsprechenden Berechtigungen verfügen, um nach Benutzern zu suchen und diese zu authentifizieren.
- **Passwort des Domänenbenutzers.** Aus Sicherheitsgründen wird das Passwort des Domänenbenutzers durch Sternchen (*) ersetzt.
- **SSL verwenden.** Geben Sie true an, um Secure Sockets für die Kommunikation mit dem Active Directory-Server zu verwenden.

Wenn Sie die gewünschten Einstellungen vorgenommen haben, klicken Sie auf Setzen.

Active Directory mit lokaler Überschreibung

Über die Sicherheits-Provider-Option “Active Directory mit lokalem Überschreiben” kann Active Directory mit den zusätzlichen Optionen eines lokalen Principal-Filters und der Möglichkeit, lokale Gruppen anzugeben, verwendet werden. Um die Einstellungen für Active Directory mit lokalem Überschreiben zu konfigurieren, klicken Sie rechts neben dem Kontrollkästchen “Active Directory mit lokalem Überschreiben” auf Einstellungen bearbeiten. Die aktuellen Einstellungen werden angezeigt. Die meisten Einstellungen entsprechen denen für Active Directory. Darüber hinaus stehen jedoch die beiden folgenden Optionen zur Verfügung:

- **Erlaubte Benutzer.** Aktiviert (true) oder deaktiviert (false) die Verwendung erlaubter Benutzer, wodurch nur Benutzer in einer lokal definierten Liste in Active Directory authentifiziert werden können.
- **Erweiterte Gruppen.** Aktiviert (true) und deaktiviert (false) die Verwendung erweiterter Gruppen, wodurch eine Gruppe von Active Directory-Benutzern definiert werden kann. Active Directory-Benutzer können diesen lokalen Gruppen zugewiesen werden.

Wenn Sie die gewünschten Einstellungen vorgenommen haben, klicken Sie auf Setzen.

IBM i

Wenn IBM® SPSS® Collaboration and Deployment Services Repository auf IBM i installiert ist, wird das IBM i-Benutzerprofilverzeichnis verwendet, um Repository-Anmeldungen zu authentifizieren. Um IBM i-Einstellungen zu konfigurieren, klicken Sie rechts neben dem Kontrollkästchen “IBM i” auf Einstellungen bearbeiten. Die aktuellen Einstellungen werden angezeigt. Folgende Einstellungen können geändert werden:

- **IBM i Server.** Der Pfad zum IBM i-System, in der Regel ein DNS-auflösbarer Name oder eine IP-Adresse. Wenn Sie IBM i-Sicherheits-Provider mit Enterprise Identity Management (EIM) verwenden, um die Einzelanmeldung für IBM® SPSS® Collaboration and Deployment Services zu aktivieren, muss dieser Wert mit dem EIM-Zielregistrierungswert übereinstimmen. Wenn der EIM-Zielregistrierungswert ein vollständig qualifizierter Name des Hosts ist, geben Sie den vollständig qualifizierten Hostnamen ein.
- **Benutzerprofil.** Das Benutzerprofil, das für Verzeichnissuchen im IBM i-System verwendet wird.

- **Paßwort.** Das Passwort für das angegebene IBM i-Profil. Aus Sicherheitsgründen wird das Passwort des Domänenbenutzers durch Sternchen (*) ersetzt.
- **EIM-Suche aktivieren.** Für IBM SPSS Collaboration and Deployment Services-Installationen mit aktivierter Einzelanmeldung zeigt der Wert `true` an, dass Enterprise Identity Management aktiviert ist.
- **EIM-Server.** Enterprise Identity Management-Host-URL.
- **EIM-Benutzer.** Der Benutzername für die Enterprise Identity Management-Host-Anmeldung.
- **EIM-Passwort.** Das Passwort für den angegebenen Enterprise Identity Management-Benutzer.

Anmerkung: Jedes IBM i-Benutzerprofil kann für Verzechnissuchen verwendet werden, aber die Liste der Profile, die zurückgegeben wird, ist nach der Berechtigung des Profils gefiltert, das für die Suche verwendet wird. Wenn Sie einen Benutzer auf QSECOFR-Ebene angeben, werden alle Profile im System zurückgegeben. Wenn Sie einen Benutzer mit weniger Berechtigungen verwenden, werden basierend auf den Sicherheitseinstellungen der Benutzerprofile weniger Profile zurückgegeben.

OpenLDAP

Um OpenLDAP-Einstellungen zu konfigurieren, klicken Sie rechts neben dem Kontrollkästchen "OpenLDAP" auf Einstellungen bearbeiten. Die aktuellen Einstellungen werden angezeigt. Folgende Einstellungen können geändert werden:

- **Host-URL.** Der Pfad zum LDAP-Server, in der Regel ein DNS-auflösbarer Name oder eine IP-Adresse (beispielsweise `ldap://`). Der Standardport für LDAP ist 389.
- **Benutzer-Basis-DN.** Basis-Distinguished-Name für Benutzersuchen.
- **Gruppen-Basis-DN.** Basis-Distinguished-Name für Gruppensuchen.
- **SearchUser.** Eine Benutzer-ID, um Suchen in einem Distinguished-Name-Format durchzuführen. Der angegebene Name muss über die entsprechenden Berechtigungen verfügen, um nach Benutzern zu suchen und diese zu authentifizieren.
- **SearchUser-Password.** Aus Sicherheitsgründen wird das Passwort des Domänenbenutzers durch Sternchen (*) ersetzt.

Wenn Sie die gewünschten Einstellungen vorgenommen haben, klicken Sie auf Setzen.

SiteMinder

Um SiteMinder-Einstellungen zu konfigurieren, klicken Sie rechts neben dem Kontrollkästchen "SiteMinder" auf Einstellungen bearbeiten. Die aktuellen Einstellungen werden angezeigt. Folgende Einstellungen können geändert werden:

- **Lokaler Computer.** IBM® SPSS® Collaboration and Deployment Services-Host-Adresse oder -Domänenname.
- **SiteMinder IP.** Server-Adresse oder Domänenname der SiteMinder-Richtlinie.
- **Agentengeheimnis.** Agentengeheimnis für den Agenten `spss-agent`; wird für die Anmeldung an den SiteMinder-Richtlinien-Server verwendet.

- **Stammverzeichnis.** Stammverzeichnis-Basis-DN, zum Beispiel DC=Domänenname Teil 1, DC=Domänenname Teil 2
- **Organisationsstamm.** Organisationsstamm, zum Beispiel OU=Einheit, DC=Domänenname Teil 1, DC=Domänenname Teil 2 ...
- **Verzeichnisserver.** Verzeichnis der Server-Adresse oder Domänenname.
- **Verzeichnis-Benutzername.** Der Name des Benutzers für die Verzeichnisanmeldung.
- **Verzeichnis-Benutzerpasswort.** Das Passwort für die Verzeichnisanmeldung.
- **Verzeichnisname.** LDAP-Verzeichnisname.
- **Benutzerabfrage für Verzeichnissuche.** LDAP-Abfrage für benutzerbasierte Authentifizierung.
- **Gruppenabfrage für Verzeichnissuche.** LDAP-Abfrage für gruppenbasierte Authentifizierung.

Wenn Sie die gewünschten Einstellungen vorgenommen haben, klicken Sie auf Setzen.

Einzelanmeldung

Einzelanmeldung (SSO) ist eine Methode für die Zugriffskontrolle, die es einem Benutzer ermöglicht, sich einmal anzumelden und Zugriff auf Ressourcen mehrerer Softwaresysteme zu erhalten, ohne sich mehrmals anmelden zu müssen. IBM® SPSS® Collaboration and Deployment Services bietet die Möglichkeit der Einzelanmeldung, bei der Benutzer zum ersten Mal durch einen externen Verzeichnisdienst wie Windows Active Directory basierend auf dem **Kerberos**-Sicherheitsprotokoll und im Folgenden anhand der Anmeldeinformationen authentifiziert werden, die in allen IBM SPSS Collaboration and Deployment Services-Anwendungen (z. B. IBM® SPSS® Collaboration and Deployment Services Deployment Manager, IBM® SPSS® Collaboration and Deployment Services Deployment Portal oder in einem Portalserver) enthalten sind, ohne dass eine zusätzliche Authentifizierung nötig ist.

Die Konfiguration der Einzelanmeldung wird auf der Registerkarte "Server-Verwaltung" von Deployment Manager durchgeführt. Beachten Sie, dass eine Reihe von Voraussetzungen erfüllt sein muss, bevor die Einzelanmeldung aktiviert werden kann. Weitere Informationen zur Installation und Konfiguration finden Sie in der IBM SPSS Collaboration and Deployment Services-Dokumentation.

Konfigurieren von Einzelanmeldungen

- Wählen Sie Server-Administration aus dem Menü "Extras", melden Sie sich bei einem IBM® SPSS® Collaboration and Deployment Services-Server an und doppelklicken Sie auf das Symbol Einzelanmeldung. Der Editor für Einzelanmeldungs-Provider wird geöffnet.

Abbildung 7-1
Editor für Einzelanmeldungs-Provider

Einzelanmeldungs-Provider-Konfiguration

	<input type="checkbox"/> Aktivieren
Sicherheits-Provider	Active Directory
KDC-Host-Adresse	kdc.mycompany.com
Kerberos-Realm	MYCOMPANY.COM
Host-Adresse	server.mycompany.com
Kerberos Service-Principal	HTTP/server.mycompany.com@MYCOMPANY.COM
Kerberos Service-Principal-Kennwort

Kerberos Key Table-URL	FILE:C:/keytab/krb5.keytab
JAAS-Konfigurationsdatei	#USE_SUPPLIED#

- **Aktivieren.** Aktiviert oder deaktiviert die Verwendung von Einzelanmeldungs-Provider.

-
- **Sicherheits-Provider.** Ein konfigurierter externer Sicherheits-Provider, wie Windows Active Directory. Lokale Sicherheits-Provider können nicht ausgewählt werden.
 - **Host-Adresse für Kerberos Key Distribution Center.** Vollständig qualifizierter Name des Kerberos-Domänencontroller-Hosts. Bei Windows Active Directory ist dies der Name des Hosts, auf dem die Microsoft Active Directory-Dienste installiert sind.
 - **Kerberos-Realm.** Der Kerberos-Realm. Bei Active Directory ist dies der Domänenname.
 - **Host.** Der Name des IBM® SPSS® Collaboration and Deployment Services Repository-Hosts. Beispiel: repositoryhost.mycompany.com.
 - **Kerberos Service-Principal-Name.** Der Benutzername für den Kerberos-Service-Principal.
 - **Kerberos Service-Principal-Passwort.** Das Passwort für den Kerberos-Service-Principal.
 - **URL zur Schlüsseltabelle für Kerberos.** Der URL zur keytab-Datei für die Kerberos-Principal-Authentifizierung.
 - **JAAS-Konfigurationsdatei.** Der Pfad der JAAS-(Java Authentication and Authorization Service-)Konfigurationsdatei auf dem IBM SPSS Collaboration and Deployment Services-Host-Dateisystem. Überschreibt, wenn angegeben, die JAAS-Standardkonfiguration. Je nach Anwendungsserver kann dies erforderlich sein, um die JRE für die Unterstützung von SSO zu konfigurieren.

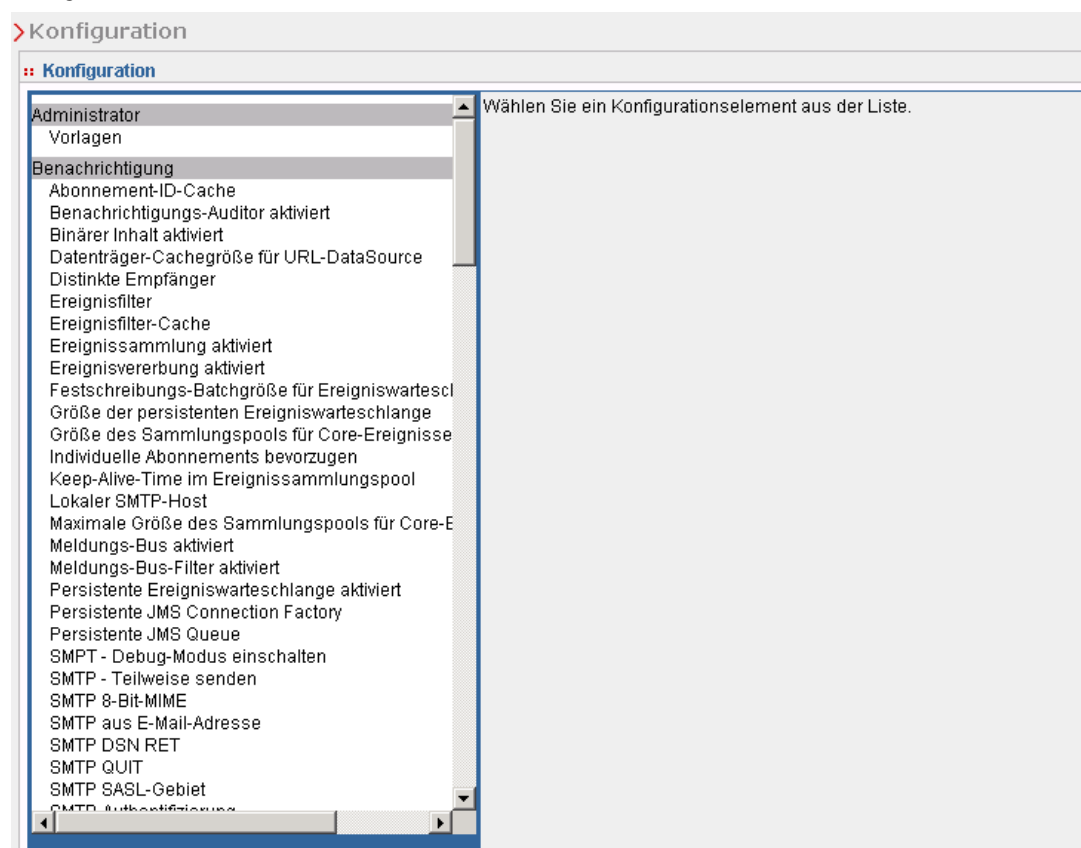
Repository-Konfiguration

IBM® SPSS® Collaboration and Deployment Services bietet eine Vielzahl von Optionen für die Konfiguration seiner Komponenten, die von den Vorlagen, die für die Benutzeroberfläche verwendet werden, bis hin zu den Meldungen reichen, die im Anmeldungsfenster erscheinen.

Führen Sie folgende Schritte im browserbasierten IBM® SPSS® Collaboration and Deployment Services Deployment Manager aus, um auf diese Optionen zuzugreifen:

- Klicken Sie in Konfiguration in der Navigationsliste. Die Konfigurationsseite wird geöffnet.

Abbildung 8-1
Konfigurationsseite



- Klicken Sie in der Konfigurationsliste auf den Link für die Eigenschaft, die Sie konfigurieren möchten.

Jeder Eigenschaftskonfigurationsbildschirm hat zwei Schaltflächen, Festlegen und Standard verwenden. Klicken Sie, nachdem Sie eine Konfiguration vorgenommen haben, auf die Schaltfläche Festlegen, damit die neue Einstellung wirksam wird. Um einen Wert auf die ursprüngliche Systemkonfiguration zurückzusetzen, klicken Sie auf die Schaltfläche Standard verwenden.

Anmerkung: Bestimmte unten aufgeführte Konfigurationsoptionen sind für optionale IBM SPSS Collaboration and Deployment Services-Komponenten oder andere SPSS Inc.-Produkte, wie IBM® SPSS® Statistics oder IBM® ShowCase®, vorgesehen. Die Optionen sind nur verfügbar, wenn die Komponenten installiert sind.

Administrator

Die Administrator-Konfigurationsoption ermöglicht es Ihnen, den Speicherort für die Vorlagen anzugeben, die verwendet werden, um die administrativen Benutzeroberflächen zu generieren. Standardmäßig verwendet das System den Pfad, der durch das Installationsprogramm festgelegt wurde.

Bearbeiten des Vorlagen-Verzeichnisses:

- ▶ Klicken Sie in der Konfigurationsliste unter “Administrator” auf Vorlagen. Das aktuelle Vorlagenverzeichnis wird im Textfeld “Vorlagen” angezeigt.
- ▶ Geben Sie im Textfeld “Vorlagen” den neuen Pfad des Verzeichnisses ein, das die Vorlagen enthält, die Sie verwenden möchten.
- ▶ Klicken Sie auf Setzen. Der von Ihnen angegebene Pfad wird zum Standardpfad für den Zugriff des Systems auf Vorlagen.
- ▶ Um den systemdefinierten Standardwert wiederherzustellen, klicken Sie auf Standard verwenden. Mit dieser Option stellen Sie das Standardverzeichnis, das bei der Installation des Systems festgelegt wurde, wieder her.

BIRT Report Designer für IBM SPSS

Die Konfigurationsoptionen von BIRT Report Designer ermöglichen die Angabe von Einstellungen, die die Verarbeitung und Anzeige von Berichten beeinflussen. Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter “BIRT Report Designer für IBM SPSS” auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-1
BIRT Report Designer for IBM SPSS-Konfigurationsoptionen

Name	Beschreibung	Einstellungen
Speicherpfad der verknüpften BIRT-Ressourcen	Das Verzeichnis auf dem Server-Dateisystem, in dem externe Ressourcen für Berichte wie Cascading Stylesheets und Bilder gespeichert werden.	Der vollständige Pfad des Verzeichnisses, das externe Ressourcen enthält. Um den systemdefinierten Standardwert wiederherzustellen, klicken Sie auf Standard verwenden. Mit dieser Option stellen Sie das Standardverzeichnis, das bei der Installation des Systems festgelegt wurde, wieder her.
SVG-Diagramm aktivieren	Gibt an, ob die SVG-Diagrammausgabe aktiviert werden soll. Diese Einstellung sollte nur ausgewählt werden, wenn SVG-Ausgabe gewünscht wird und die Browser, die die Berichts Ausgabe anzeigen, SVG-fähig sind. Wenn diese Option nicht ausgewählt ist, verwenden Berichte das PNG-Bildformat anstelle von SVG.	Standardmäßig deaktiviert.

Cache-Provider

Die Cache-Provider-Option ermöglicht Ihnen die Angabe und Konfiguration der Daten-Cache-Provider-Klasse. Standardmäßig wird Ehcache (*com.spss.cache.service.ehcache.EhcacheProvider*) verwendet. In geclusterten IBM® SPSS® Collaboration and Deployment Services-Installationen erlauben zusätzliche Optionen, Ehcache für automatische Erkennung von Peers zu konfigurieren, die mithilfe einer Multicast-Gruppe an einem Cluster teilnehmen.

Alternativ kann auch Oracle Coherence als IBM® SPSS® Collaboration and Deployment Services Repository-Cache verwendet werden. So aktivieren Sie Oracle Coherence:

- ▶ Erwerben und lizenzieren Sie die Coherence-Komponenten von Oracle. Coherence*. *jar*-Dateien müssen in das *<IBM SPSS Collaboration and Deployment Services-Installationsverzeichnis>/components/cache-provider* gelegt werden.
- ▶ Installieren Sie *coherence_cache_provider.package* aus dem Ordner *optional* auf dem IBM SPSS Collaboration and Deployment Services-Installationsdatenträger.
- ▶ Geben Sie *com.spss.cache.service.coherence.CoherenceCacheProvider* als Cache-Provider in den Konfigurationseinstellungen an.

Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter “Cache-Provider” auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Name	Beschreibung	Einstellungen
Cache-Provider-Klassenname	Cache-Provider-Klassenname.	Name der Klasse.
Multicast-Gruppenadresse	Die Multicast-Gruppenadresse für Ehcache.	Gültige Netzwerkadresse.
Multicast-Gruppenport	Für Ehcache ein dedizierter Port für die den Multicast-Heartbeat-Verkehr.	Gültige Portnummer.
Standardwerte überschreiben	Wenn die Option aktiviert ist, verwendet der Provider für Ehcache Werte der <i>Multicast-Gruppenadresse</i> und <i>Multicast-Gruppenport</i> , um die Standards zu überschreiben.	Standardmäßig deaktiviert.

Benutzerdefinierte Dialogfelder

Sofern verfügbar können Sie mit den Optionen für die Konfiguration benutzerdefinierter Dialogfelder in IBM® SPSS® Statistics Einstellungen für die Ausführung benutzerdefinierter Dialogfelder angeben.

Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter “Benutzerdefiniertes Dialogfeld” auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-2
Konfigurationsoptionen für benutzerdefinierte Dialogfelder

Name	Beschreibung	Einstellungen
Durchsuchen des Dateiservers aktiviert	Legt fest, ob bei der Auswahl eines Daten-Sets für ein benutzerdefiniertes Dialogfeld das Durchsuchen nach SPSS Statistics-Daten-Sets auf dem angegebenen Dateiserver aktiviert ist.	Markieren Sie diese Option, um sie zu aktivieren.
Speicherort des Dateiservers	Der Speicherort eines (Repository-externen) Dateiservers, der bei der Auswahl eines Daten-Sets für ein benutzerdefiniertes Dialogfeld für das Durchsuchen nach SPSS Statistics-Daten-Sets verwendet wird. Wenn das Durchsuchen des Dateiservers aktiviert und kein Speicherort angegeben ist, wird das Dateisystem des angegebenen SPSS Statistics-Servers verwendet.	Bei dem Wert kann es sich um einen Netzwerkpfad oder um den absoluten Pfad eines Verzeichnisses handeln.

Name	Beschreibung	Einstellungen
Name des Dateiservers	Der Name, der dem für das Durchsuchen nach SPSS Statistics-Daten-Sets zu verwendenden Dateiserver zugewiesen werden soll.	Ein String-Wert (Zeichenfolge). Wenn kein Wert angegeben ist, wird der Name "File Server" verwendet.
Durchsuchen des Repository aktiviert	Legt fest, ob bei der Auswahl eines Daten-Sets für ein benutzerdefiniertes Dialogfeld das Durchsuchen nach SPSS Statistics-Daten-Sets im Repository aktiviert ist.	Standardmäßig aktiviert.
SPSS Statistics-Server	Der Repository-Name oder URI eines SPSS Statistics-Servers, der für die Ausführung der Syntax für ein benutzerdefiniertes Dialogfeld verwendet wird. Alternativ kann der Name oder URI eines Server-Clusters angegeben werden. In diesem Fall wird automatisch nach Verfügbarkeit ein Server aus dem Cluster ausgewählt. Wenn kein Server angegeben ist, wird der Standardserver ausgewählt, indem ein verfügbarer Server aus der ersten gültigen Server-Cluster-Definition verwendet wird. Wenn keine gültigen Cluster gefunden werden, wird der erste gefundene, gültige Server verwendet.	Eine Zeichenkette, die dem Repository-Namen oder URI des Serverobjekts entspricht, zum Beispiel <code>spsscr:///id=0a30063bc975ede400</code> . Den URI finden Sie in den Objekteigenschaften. Weitere Informationen finden Sie in der IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Dokumentation.
SPSS Statistics-Serveranmeldedaten	Die Anmeldeinformationen, über die eine Verbindung mit dem SPSS Statistics-Server hergestellt wird, wenn Syntax für ein benutzerdefiniertes Dialogfeld ausgeführt wird. <i>Hinweis:</i> Die Anmeldeinformationen sind nicht erforderlich, wenn Active Directory für die Verwendung mit IBM® SPSS® Collaboration and Deployment Services konfiguriert wurde.	Eine Zeichenkette, die dem Repository-Namen oder URI des Credential-Objekts entspricht.
SPSS Statistics-Sitzungs-Zeitüberschreitung	Legt den Zeitüberschreitungswert in Minuten fest, der angibt, wie lange eine Verbindung zum SPSS Statistics-Server aufrechterhalten werden soll, wenn keine Aktivität seitens eines Benutzers erfolgt.	Ganzzahl. Die Standardeinstellung lautet 20 (Minuten).

Datenservice

Die Datenservice-Konfigurationsoptionen ermöglichen die Angabe von Parametern zur Optimierung der Datenservice-Verbindungen.

Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter “Datenservice” auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-3
Datenservice-Konfigurationsoptionen

Name	Beschreibung	Einstellungen
Aktive Verbindungen - maximale Anzahl	Maximale Anzahl an aktiven Verbindungen.	Ganzzahl. Die Standardeinstellung lautet 5.
Inaktive Verbindungen - maximale Anzahl	Maximale Anzahl an inaktiven Verbindungen.	Ganzzahl. Die Standardeinstellung lautet 5.

Deployment Manager

Die Deployment Manager-Konfigurationsoption ermöglicht es Ihnen, die Protokoll-Zeitbeschränkung für die Kommunikation zwischen IBM® SPSS® Collaboration and Deployment Services Deployment Manager und dem Repository anzugeben. Geben Sie die Zeit, die der Deployment Manager-Client auf einen Repository-Server warten soll, in Sekunden an. Verwenden Sie einen höheren Wert, wenn bei Server-Transaktionen Fehlermeldungen gegeben werden.

Bearbeiten der Protokoll-Zeitbeschränkung:

- ▶ Klicken Sie in der Konfigurationsliste unter “Deployment Manager” auf Protokoll-Zeitbeschränkung. Der aktuelle Wert wird angezeigt.
- ▶ Geben Sie im Textfeld “Protokoll-Zeitbeschränkung” die gewünschte Anzahl von Sekunden ein.
- ▶ Klicken Sie auf Setzen. Der von Ihnen angegebene Wert wird als Zeitbeschränkung übernommen.
- ▶ Um den systemdefinierten Standardwert wiederherzustellen, klicken Sie auf Standard verwenden. Mit dieser Option stellen Sie den Standardwert, der bei der Installation des Systems festgelegt wurde, wieder her.

Deployment Portal

Die Konfigurationsoptionen von Deployment Portal ermöglichen es Ihnen, Authentifizierungseinstellungen und die Bericht-Zeitüberschreitungsgrenze für die webbasierte IBM® SPSS® Collaboration and Deployment Services Deployment Portal-Anwendung anzugeben.

Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter Deployment Portal auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-4
IBM SPSS Collaboration and Deployment Services Deployment Portal-Konfigurationsoptionen

Name	Beschreibung	Einstellungen
Konfigurierte Authentifizierungskriterienklasse	Der Name der Java-Klasse, der verwendet wird, um Authentifizierungsinformationen für die Deployment Portal-Anwendung bereitzustellen. Der Standardwert ist <i>com.spss.er.internal.configuration.ConfiguredAuthenticationImpl</i> und die Einstellung wird im Klassenpfad des Anwendungsservers vorgenommen. Die Klasse muss der Authentifizierungsschnittstelle entsprechen, die von Deployment Portal bereitgestellt wird (<i>com.spss.er.internal.configuration.ConfiguredAuthenticationInterface.java</i>).	Name der Klasse.
Konfigurierte Authentifizierungskriterien verwenden	Ermöglicht es dem Benutzer, Authentifizierungsinformationen über konfigurierte Authentifizierungskriterien an Deployment Portal weiterzugeben und so die Anmeldemaske zu umgehen.	Standardmäßig deaktiviert.

Deployment Portal-Scoring

Mit der Konfigurationsoption "Batch-Scoring-Zeilengrenze" können Sie die maximale Anzahl von Zeilen angeben, die beim Batch-Scoring aus einem ausgewählten Daten-Set verwendet wird.

So ändern Sie die Zeilengrenze:

- ▶ Klicken Sie in der Konfigurationsliste unter "Deployment Portal-Scoring" auf Batch-Scoring-Zeilengrenze. Der aktuelle Wert wird angezeigt.
- ▶ Geben Sie im Textfeld "Batch-Scoring-Zeilengrenze" die gewünschte Anzahl von Zeilen ein.
- ▶ Klicken Sie auf Setzen. Der von Ihnen angegebene Wert wird als Zeitbeschränkung übernommen.
- ▶ Um den systemdefinierten Standardwert wiederherzustellen, klicken Sie auf Standard verwenden. Mit dieser Option stellen Sie den Standardwert, der bei der Installation des Systems festgelegt wurde, wieder her.

Enterprise-Ansicht

Die Enterprise-Ansicht-Konfigurationsoptionen ermöglichen die Angabe von Einstellungen zur Verwendung eines IBM® SPSS® Statistics-Datendatei-Servers. Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter Enterprise-Ansicht auf die entsprechende

Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-5

IBM SPSS Collaboration and Deployment Services Enterprise View-Konfigurationsoptionen

Name	Beschreibung	Einstellungen
Maximale CQL-Abfragespalten	Die maximale Zeilenzahl, die von CQL (Common Query Language)-Abfragen zurückgegeben wird.	Ganzzahl. Die Standardeinstellung lautet 2.
SPSS Statistics Data File Additional Servers	Mithilfe dieser Einstellung werden zusätzliche SPSS Statistics-Datendatei-Server angegeben, mit denen sich Metadaten aus SPSS Statistics-Datendateien abrufen lassen.	Eine durch Semikolon getrennte Liste mit host:port-Werten, z. B. server2:18886;server3:18886
SPSS Statistics Data File Load Balance	Die Lastenausgleichseinstellung steuert, ob beim Abruf von Metadaten aus SPSS Statistics-Datendateien mehrere SPSS Statistics-Datendatei-Server im ausfallsicheren Modus oder Lastenausgleichsmodus verwendet werden. Im ausfallsicheren Modus werden die Listenserver in sequenzieller Reihenfolge verwendet. Wenn der erste nicht funktioniert, wird der zweite verwendet usw. Wenn der Lastenausgleich aktiviert wird, wird einer der verfügbaren Server nach dem Zufallsprinzip ausgewählt. Diese Einstellung hat keine Wirkung, sofern keine zusätzlichen SPSS Statistics-Datendatei-Server angegeben werden.	Standardmäßig aktiviert.
SPSS Statistics Data File Server Host	Der Name des SPSS Statistics-Datendatei-Servers, der zum Zugriff auf SPSS Statistics-Datendateien verwendet wird. Falls kein Host angegeben ist, wird der localhost verwendet.	Eine gültige IP-Adresse bzw. ein gültiger Hostname.
SPSS Statistics Data File Server Port	Der Port für den SPSS Statistics-Datendatei-Server. Falls kein Port angegeben ist, wird der Standard-Port verwendet.	Eine gültige Portnummer.
SPSS Statistics Data File Server Secure	Indikator, ob bei der Kommunikation mit dem SPSS Statistics-Datendatei-Server SSL verwendet werden soll oder nicht. Der Standardwert "false" heißt, dass keine Secure Sockets verwendet werden.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".

Hilfe

Die Hilfe-Konfigurationsoption ermöglicht es Ihnen, den Speicherort des Hilfesystems für IBM® SPSS® Collaboration and Deployment Services Deployment Manager anzugeben. Standardmäßig verwendet das System den Pfad, der durch das Installationsprogramm festgelegt wurde.

Bearbeiten des Hilfeverzeichnis:

- ▶ Klicken Sie in der Konfigurationsliste unter “Hilfe” auf Verzeichnis. Das aktuelle Hilfeverzeichnis wird im Textfeld “Hilfe” angezeigt.
- ▶ Geben Sie im Textfeld “Hilfe” den Pfad des Verzeichnisses ein, das das Hilfesystem enthält.
- ▶ Klicken Sie auf Setzen. Der von Ihnen angegebene Pfad wird zum Standardpfad für den Zugriff des Systems auf die Onlinehilfe.
- ▶ Um den systemdefinierten Standardwert wiederherzustellen, klicken Sie auf Standard verwenden. Mit dieser Option stellen Sie das Standardverzeichnis, das bei der Installation des Systems festgelegt wurde, wieder her.

Benachrichtigung

Mit den Konfigurationsoptionen für Benachrichtigungen können Sie SMTP-Mail-Einstellungen angeben und die Abstimmung der Leistung des Benachrichtigungsdienstes aktivieren. Für weitere Informationen siehe Thema [Optimieren der Leistung des Benachrichtigungsdienstes](#) in Kapitel 11 auf S. 105. Sie können auch Syndication-Einstellungen für Feeds vom Typ RSS (Really Simple Syndication) angeben.

Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter “Benachrichtigung” auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-6
Konfigurationsoptionen für Benachrichtigungen

Name	Beschreibung	Einstellungen
Binärer Inhalt aktiviert	Aktiviert binäre Inhalte, z. B. E-Mail-Anhänge, für Benachrichtigungsmeldungen.	Standardmäßig aktiviert.
Größe des Sammlungs-pools für Core-Ereignisse	Anzahl der Threads, die im Ereignissammlungspool bleiben, auch wenn sie inaktiv sind.	Ganzzahl. Die Standardeinstellung lautet 16.

Name	Beschreibung	Einstellungen
Distinkte Empfänger	Falls das Kontrollkästchen aktiviert ist, werden Benachrichtigungsmeldungen nur für eindeutige Empfänger generiert. Anderenfalls werden die doppelten Adressen nicht entfernt und die Empfänger erhalten Meldungen, die von all ihren einzelnen Abonnements und Benachrichtigungen generiert wurden, die dem bestimmten Benachrichtigungsereignis entsprechen. Diese Option sollte nur zu Debug-Zwecken geändert werden.	Standardmäßig aktiviert.
Ereignissammlung aktiviert	Definiert, ob Benachrichtigungsereignisse durch den Service verarbeitet werden sollen.	Standardmäßig aktiviert.
Keep-Alive-Time im Ereignissammlungspool	Wenn die Anzahl an Threads die Core-Anzahl der Threads im Ereignissammlungspool überschreitet, ist dies die maximale Dauer in Sekunden, die überzählige inaktive Threads auf neue Ereignisse warten, bevor sie beendet werden.	Ganzzahl. Die Standardeinstellung lautet 32.
Ereignisvererbung aktiviert	Definiert, ob abgeleitete Benachrichtigungsereignisse durch den Service verarbeitet werden sollen.	Standardmäßig deaktiviert.
Ereignisfilter	Filtert Benachrichtigungsereignisse heraus, die zu einem frühen Zeitpunkt im Prozess über keine entsprechenden Abonnements bei zugehörigen Benachrichtigungs-Providern oder Abonnenten verfügen.	Wahr oder Falsch. Die Standardeinstellung lautet "wahr".
Ereignisfilter-Cache	Definiert eine maximale Größe des LRU-Cache, der während der Ereignisfilterung verwendet werden soll.	Ganzzahl. Die Standardeinstellung lautet 2048.
Stringschlüssel für Ereignisfilter	Verwendet Strings anstelle von Hash-Codes zur Identifizierung von Benachrichtigungsereignissen.	Standardmäßig deaktiviert.
Festschreibungs-Batchgröße für Ereigniswarteschlangenspeicher	Legt die Festschreibungs-Batchgröße des persistenten Speichers für die ankommenden Benachrichtigungsereignisse fest. Der Benachrichtigungsservice muss neu gestartet werden, damit die Änderungen wirksam werden.	Ganzzahl. Die Standardeinstellung lautet 32.

Name	Beschreibung	Einstellungen
Maximale Größe des Sammlungspools für Core-Ereignisse	Die maximal zulässige Anzahl an Threads im Ereignissammlungspool.	Ganzzahl. Die Standardeinstellung lautet 32.
Meldungs-Bus aktiviert	Definiert, ob Benachrichtigungsmeldungen an den JMS-Meldungs-Bus gesendet werden sollen.	Standardmäßig aktiviert.
Meldungs-Bus-Filter aktiviert	Definiert, ob nur Benachrichtigungen von Interesse an den JMS-Meldungs-Bus gesendet werden sollen.	Standardmäßig aktiviert.
Benachrichtigungs-Auditor aktiviert	Legt fest, ob der Benachrichtigungsservice mit dem Auditing-Service verknüpft werden soll.	Standardmäßig aktiviert.
Benachrichtigungs-Cache verteilt	Legt fest, ob der Benachrichtigungsservice einen verteilten Cache verwenden soll. Der Benachrichtigungsservice muss neu gestartet werden, damit die Änderungen wirksam werden.	Standardmäßig deaktiviert.
Warteschlange für Benachrichtigungen	Stellt ankommende Benachrichtigungsereignisse in die Warteschlange, bis sie durch Hintergrund-Threads verarbeitet werden können.	Wahr oder Falsch. Die Standardeinstellung lautet "wahr".
Persistente Ereigniswarteschlange aktiviert	Definiert, ob eingehende Benachrichtigungsereignisse temporär im persistenten Speicher auf dem Datenträger bleiben sollen, um die Menge des belegten Speichers zu minimieren. Der Benachrichtigungsservice muss neu gestartet werden, damit die Änderungen wirksam werden.	Standardmäßig deaktiviert.
Größe der persistenten Ereigniswarteschlange	Legt die maximale Größe des persistenten Speichers für die ankommenden Benachrichtigungsereignisse fest (in Megabyte). Der Benachrichtigungsservice muss neu gestartet werden, damit die Änderungen wirksam werden.	Ganzzahl. Die Standardeinstellung lautet 8 MB.
Typ der persistenten Ereigniswarteschlange	Definiert den Speichertyp für die persistente Ereigniswarteschlange. Der Benachrichtigungsservice muss neu gestartet werden, damit die Änderungen wirksam werden.	Entweder DISK oder JMS. Standard ist DISK.

Name	Beschreibung	Einstellungen
Persistente JMS Connection Factory	Definiert einen JNDI-Namen für JMS Connection Factory für fortbestehende ankommende Benachrichtigungsereignisse. Der Benachrichtigungsservice muss neu gestartet werden, damit die Änderungen wirksam werden.	Eine deploymentspezifische und/oder serverspezifische Zeichenfolge, bei der zwischen Groß- und Kleinschreibung unterschieden wird und die vom JNDI-Service verwendet wird, um die JMS Connection Factory zu kennzeichnen.
Persistente JMS Queue	Definiert einen JNDI-Namen für JMS Queue für fortbestehende ankommende Benachrichtigungsereignisse. Der Benachrichtigungsservice muss neu gestartet werden, damit die Änderungen wirksam werden.	Eine deploymentspezifische und/oder serverspezifische Zeichenfolge, bei der Groß- und Kleinschreibung beachtet wird und die vom JNDI-Service verwendet wird, um die JMS-Queue zu kennzeichnen.
Individuelle Abonnements bevorzugen	Wenn dieses Kontrollkästchen aktiviert ist, hat die Verarbeitung der Abonnements bei Benutzern Vorrang, deren Einstellungen für individuelle Abonnements und die vom Administrator eingestellten Benachrichtigungen identisch sind. Wenn das Kontrollkästchen deaktiviert wird, kehrt sich die Verarbeitungsreihenfolge um.	Standardmäßig aktiviert.
SMTP 8-Bit-MIME	Wenn die Option auf "wahr" gesetzt ist und der Server die Erweiterung 8BITMIME unterstützt, werden Textteile mit "quoted-printable"- oder "base64"-Kodierungen in "8bit"-Kodierung konvertiert, falls sie die RFC2045-Regeln für 8-Bit-Text einhalten.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".
SMTP-Authentifizierung	Wenn die Option auf "wahr" gesetzt ist, wird versucht, den Benutzer mithilfe des Befehls AUTH zu authentifizieren.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".
Zeitüberschreitung der SMTP-Verbindung	Zeitbegrenzungswert für Socket-Verbindung in Millisekunden.	Ganzzahl. Der Standardwert für die Zeitbeschränkung lautet "unendlich".
SMTP-Distributor aktiviert	Wenn dieses Kontrollkästchen aktiviert ist, ist eine Verteilung von Benachrichtigungsmeldungen über SMTP möglich. Der Repository-Administrator kann die SMTP-Verteilung deaktivieren, um alle vom Server generierten E-Mails zu unterdrücken. Beachten Sie, dass bei deaktivierter SMTP-Verteilung alle Nachrichten verloren gehen, da das Repository keine generierten E-Mail-Nachrichten speichert.	Standardmäßig aktiviert.

Name	Beschreibung	Einstellungen
SMTP DSN Notify	Die Option NOTIFY für den Befehl RCPT für DSN (Delivery Status Notifications, RFC3461).	Entweder NEVER oder eine Kombination aus SUCCESS, FAILURE und DELAY (durch Kommas getrennt).
SMTP DSN RET	Die Option RET für den Befehl MAIL für DSN (Delivery Status Notifications, RFC3461).	Entweder FULL oder HDRS.
SMTP EHLO	Wenn "falsch" eingestellt ist, wird nicht versucht, eine Anmeldung mit dem EHLO-Befehl durchzuführen.	Wahr oder Falsch. Die Standardeinstellung lautet "wahr".
SMTP aus E-Mail-Adresse	Absender- oder Antwortadresse bei der Verwendung für Benachrichtigungs-E-Mails.	Eine vorhandene SMTP-E-Mail-Adresse.
SMTP-Host	Der Hostname bzw. die IP-Adresse des SMTP-Servers, der zum Versenden von Mails verwendet wird.	Eine gültige IP-Adresse bzw. ein gültiger Hostname.
Lokaler SMTP-Host	Name des lokalen Hosts, der im SMTP-Befehl HELO oder EHLO verwendet wird. Verwendet standardmäßig <i>InetAddress.getLocalHost().getHostName()</i> . Muss für gewöhnlich nicht eingestellt werden, wenn Ihr JDK und Ihr Name-Service korrekt konfiguriert sind.	Eine gültige IP-Adresse bzw. ein gültiger Hostname.
SMTP-Password	Passwort für die SMTP-Authentifizierung.	Maskiertes Passwort.
SMTP-Port	Der Port, der für ausgehende Mails verwendet wird.	Eine gültige Portnummer. Die Standardeinstellung lautet 25.
SMTP QUIT	Wenn diese Option auf "wahr" eingestellt ist, wartet der Transport die Antwort auf den Befehl QUIT ab. Wenn diese Option auf "falsch" eingestellt ist, wird der Befehl QUIT gesendet und die Verbindung sofort geschlossen.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".
SMTP SASL-Gebiet	Das SASL-Gebiet (Simple Authentication and Security Layer) zur Verwendung mit DIGEST-MD5-Authentifizierung.	Eine deploymentspezifische und/oder serverspezifische Zeichenkette, die das Gebiet oder die Domäne kennzeichnet, aus dem/der der Principal-Name ausgewählt werden sollte.

Name	Beschreibung	Einstellungen
SMTP - Teilweise senden	Wenn diese Option auf "wahr" eingestellt ist und eine Nachricht einige gültige und einige ungültige Adressen verwendet, wird die Meldung dennoch gesendet und der teilweise Misserfolg durch eine <i>SendFailedException</i> gemeldet. Wenn die Option auf "falsch" eingestellt ist, wird die Meldung an keinen der Empfänger gesendet, wenn eine oder mehrere der Empfängeradressen ungültig sind.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".
SMTP-Zeitüberschreitung	Zeitbegrenzungswert für Socket-E/A in Millisekunden.	Ganzzahl. Der Standardwert für die Zeitbeschränkung lautet "unendlich".
SMTP-Transferprotokoll	Meldungstransferprotokoll.	Entweder smtp oder smtps. Der Standardwert lautet smtp, während smtps für Verbindungen zum entsprechenden Dienst über SSL/TLS verwendet wird.
SMTP - Debug-Modus einschalten	Schaltet den Debug-Modus ein und aus.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".
SMTP-Benutzer	Standard-Benutzername für SMTP.	Benutzername.
Abonnement-ID-Cache	Definiert eine maximale Größe des LRU-Cache für häufig verwendete Abonnement-IDs.	Ganzzahl. Die Standardeinstellung lautet 2048.
Cache-TTL für gesammelte Einträge	Definiert die Zeitspanne, für die gesammelte Feed-Einträge im Cache abgelegt werden (in Minuten). Dies bezieht sich beispielsweise auf Feeds vom Typ RSS.	Ganzzahl. Die Standardeinstellung lautet 15 Minuten.
Höchstzahl für gesammelte Einträge	Definiert die maximale Anzahl an Einträgen in gesammelten Feeds wie RSS.	Ganzzahl. Die Standardeinstellung lautet 256.
Persistente TTL für gesammelte Einträge	Definiert die Zeitspanne, für die gesammelte Einträge im persistenten Speicher abgelegt werden (in Tagen). Dies bezieht sich beispielsweise auf Feeds vom Typ RSS.	Ganzzahl. Die Standardeinstellung lautet 7 Tage.
Typ der gesammelten Feeds	Definiert das Format der gesammelten Feeds.	Entweder RSS_2_0 oder ATOM_1_0. Die Standardeinstellung lautet RSS_2_0.
Syndication-Distributor aktiviert	Aktiviert den Syndication-Distributor für XML-Feeds.	Standardmäßig aktiviert.

Name	Beschreibung	Einstellungen
Syndication Vacuumer aktiviert	Aktiviert Syndication Vacuumer. Syndication Vacuumer löscht abgelaufene gesammelte Einträge aus dem System. Syndication Vacuumer wird basierend auf den in der Option "Syndication Vacuumer-Häufigkeit" angegebenen Intervallen automatisch ausgeführt und verwendet den Wert "Persistente TTL für gesammelte Einträge", um zu ermitteln, welche Daten abgelaufen sind und gelöscht werden können. Wenn Syndication Vacuumer nicht häufig genug ausgeführt wird, kann sich dies deutlich negativ auf die Leistungsfähigkeit der Anwendung auswirken. Das Deaktivieren dieser Option ist nicht empfehlenswert.	Standardmäßig aktiviert.
Syndication Vacuumer-Häufigkeit	Definiert die Häufigkeit (in Minuten), mit der Syndication Vacuumer ausgeführt wird. Damit Änderungen in Kraft treten, muss der Benachrichtigungsservice neu gestartet werden.	Ganzzahl. Die Standardeinstellung lautet 60 Minuten.
Syndication Vacuumer – Master	Definiert, ob Syndication Vacuumer nur auf dem Master-Knoten im Server-Cluster ausgeführt wird.	Standardmäßig deaktiviert.
Syndication Vacuumer-Quote	Schränkt die Anzahl der gesammelten Einträge ein, die während einer einzelnen Ausführung von Syndication Vacuumer gelöscht werden.	Ganzzahl. Die Standardeinstellung lautet 4096.
Datenträger-Cachegröße für URL-DataSource	Maximale Datenträger-Cachegröße für binäre Inhalte (Anhänge), die als Teil eines Benachrichtigungsereignisses gesendet werden.	Ganzzahl. Die Standardeinstellung lautet 64.

Pager

Über die Konfigurationsoption "Pager-Zeitbeschränkung" können Sie die Zeit in Minuten angeben, über die ausgelagerte Daten verfügbar sind. Das Ändern dieses Werts kann sich auf die Leistung des Paging-Systems auswirken. Ein Neustart des Repository ist nötig, damit der neue Optionswert wirksam wird.

Bearbeiten der Pager-Zeitbeschränkung:

- Klicken Sie in der Konfigurationsliste unter "Pager" auf Pager-Zeitbeschränkung. Der aktuelle Wert wird angezeigt.

- ▶ Geben Sie im Textfeld “Pager-Zeitbeschränkung” die gewünschte Anzahl von Minuten ein.
- ▶ Klicken Sie auf Setzen. Der von Ihnen angegebene Wert wird als Zeitbeschränkung übernommen.
- ▶ Um den systemdefinierten Standardwert wiederherzustellen, klicken Sie auf Standard verwenden. Mit dieser Option stellen Sie den Standardwert, der bei der Installation des Systems festgelegt wurde, wieder her.

Prozessmanagement

Die Prozessmanagement-Konfigurationsoptionen ermöglichen es Ihnen, Jobausführungseinstellungen anzugeben und die Webdienst-Endpunkte zu definieren.

Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter “Prozessmanagement” auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-7
Prozessmanagement-Konfigurationsoptionen

Name	Beschreibung	Einstellungen
Kalender-Pool	Die Wartezeit, bis der Prozessmanagement-Server das Repository erneut nach Kalenderzeitplänen absucht. Kalenderzeitpläne werden auf Basis der eingestellten Zeit/des eingestellten Datums ausgeführt.	Ganzzahl, welche die Dauer in Sekunden angibt. Die Standardeinstellung lautet 60.
Gleichzeitig inaktiv	Anzahl an Sekunden, die ein Thread inaktiv sein kann, bevor er aus dem Pool entfernt wird. Threads werden nicht entfernt, wenn damit die Poolgröße unter das Gleichzeitigkeitsminimum fallen würde.	Ganzzahl, welche die Dauer in Sekunden angibt. Die Standardeinstellung lautet 600.
Limit für Gleichzeitigkeit	Maximale Anzahl an Threads, die gleichzeitig aktiv sein können. Beachten Sie, dass jede aktiv laufende Tätigkeit (z. B. DBQ) einen Thread verbraucht.	Ganzzahl. Die Standardeinstellung lautet 25.
Gleichzeitigkeit Minimum	Die maximal zulässige Anzahl an Threads, die im Thread-Pool erstellt werden können.	Ganzzahl. Die Standardeinstellung lautet 5.
Name der JMS Connection Factory	Der Name, der für die JMS Connection Factory beim JNDI-Service registriert ist. Ziehen Sie ihre Anwendungsserver- oder JMS-Server-Dokumentation zu Rate, um den angemessenen Wert zu ermitteln.	Die Standardeinstellung lautet ConnectionFactory. Der Name muss innerhalb des zugehörigen Nachrichten-Providers eindeutig sein.

Name	Beschreibung	Einstellungen
JMS Naming Factory	Die JMS-Java-Klasse. Zum Beispiel ist die Naming-Factory für den JBoss-Anwendungsserver <i>org.jnp.interfaces.NamingContextFactory</i> . Die Einstellung kann festgelegt werden, wenn alle Meldungen für alle meldungsbasierten Jobs von einem einzigen Remote-Server stammen.	Der Standardwert ist der Klassenname der JMS Naming Factory des lokalen Anwendungsservers.
JMS Naming Service	Der URI-Speicherort des Naming-Service. Zum Beispiel ist die Naming Factory für den JBoss-Anwendungsserver <i>jnp://localhost:1099</i> . Die Einstellung kann festgelegt werden, wenn alle Meldungen für alle meldungsbasierten Jobs von einem einzigen Remote-Server stammen.	Der Standardwert ist der JMS Naming Service-URI des lokalen Anwendungsservers.
JMS-Prozessereignis-Connection Factory	Für die Prozessereigniswarteschlange verwendeter Klassenname der JMS Connection Factory.	Der Standardwert ist der Klassenname der JMS Naming Factory des lokalen Anwendungsservers.
JMS-Prozessereigniswarteschlange	JNDI-Name der JMS-Prozessereigniswarteschlange.	Der Standardwert ist die JMS-Prozessereigniswarteschlange des lokalen Anwendungsservers.
Maximale Anzahl an Iterationen	Die maximale Anzahl von Iterationen für iterative Jobschritte.	Ganzzahl. Die Standardeinstellung lautet 250.
Meldungsabfrage	Die Wartezeit (in Sekunden), bevor der Process Management-Server das Repository erneut nach meldungsbasierten Zeitplänen absucht, die aktiviert werden sollten.	Ganzzahl. Die Standardeinstellung lautet 120.
Prozessbenachrichtigung aktiviert	Gibt an, ob der Process Management-Server mit dem Benachrichtigungsserver kommunizieren soll.	Wahr oder Falsch. Standard ist wahr.
Ablaufzeit für übergebene Arbeit	Die Ablaufzeit für übergebene Jobs (in Tagen).	Ganzzahl. Die Standardeinstellung lautet 5.
Zeitstempel für übergebene Arbeit	Zeitstempelformat, das für Ordner mit übergebener Arbeit verwendet wird.	Format für Jahr, Monat, Tag, Stunde, Minute, Sekunde: yyyy.MM.dd.hh.mm.ss.SSS.
Datums- und Zeitformat für die Ordner mit Zeitstempel.	Datums- und Zeitformat für die Ordner mit Zeitstempel.	Format für Jahr, Monat, Tag, Stunde, Minute, Sekunde: yyyy.MM.dd.hh.mm.ss.SSS.
Datumsformat für die Ordner mit Zeitstempel.	Datumsformat für die Ordner mit Zeitstempel.	Monat, Tag und Jahr: MM-dd-yyyy.
Zeitformat für die Ordner mit Zeitstempel.	Zeitformat für die Ordner mit Zeitstempel.	Format für Stunde, Minute und Sekunde: HH.mm.ss.

Reporting

Die Reporting-Konfigurationsoption ermöglicht es Ihnen, den Pfad für die Ausgabe von Debug-Informationen (als XML-Datei) für die Visualisierungsverarbeitung anzugeben.

Wichtig: Falls kein Wert für diese Option angegeben wird, findet keine Generierung von Debug-Informationen für die Visualisierungsverarbeitung statt.

Bearbeiten des Verzeichnispfads:

- ▶ Klicken Sie in der Konfigurationsliste unter “Reporting” auf Vollständiges Visualisierungsverzeichnis. Das aktuelle Verzeichnis wird im Textfeld “Vollständiges Visualisierungsverzeichnis” angezeigt.
- ▶ Geben Sie den neuen Wert des absoluten Pfads des Verzeichnisses ein.
- ▶ Klicken Sie auf Setzen. Der von Ihnen angegebene Pfad wird zum Standardverzeichnis für die Ausgabe von Informationen zur Visualisierungsverarbeitung.

Repository

Die Repository-Konfigurationsoptionen ermöglichen es Ihnen, die Webdienst-Endpunkte zu definieren und die Verbindungsvalidierung zu aktivieren bzw. zu deaktivieren. Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter “Repository” auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-8
Repository-Konfigurationsoptionen

Name	Beschreibung	Einstellungen
Grenze für kategoriale Werte	Begrenzt die Zahl der kategorialen Variablenwerte, die als IBM® SPSS® Modeler-Stream-Metadaten gespeichert werden. Die gespeicherten Werte werden in den Inhalt aufgenommen, der bei der Durchführung von Suchvorgängen ausgewertet wird. Die Begrenzung ist nötig, um Zeit beim Speichern von Streams im Repository und bei der Durchführung von Suchvorgängen zu sparen.	Ganzzahl. Der Wert –1 bedeutet, dass keine Grenze vorliegt. Alle kategorialen Werte werden als Metadaten gespeichert. Geben Sie 0 ein, um das Speichern von Werten zu deaktivieren. Geben Sie 1 oder eine höhere Zahl ein, um die Zahl der gespeicherten Werte zu begrenzen.
Content-Repository-Endpunkt	Definiert die Webservice-Endpunktadresse für das Repository.	URL.

Name	Beschreibung	Einstellungen
Anmeldepaswörter müssen verschlüsselt sein	Anmeldepaswörter müssen verschlüsselt sein. "Falsch" gibt an, dass Passwörter als unverschlüsselter Text übergeben werden dürfen. <i>Anmerkung:</i> Diese Option ist für IBM® SPSS® Collaboration and Deployment Services-Deployments, bei denen SSL bereits aktiviert ist, redundant und sollte nur in Nicht-SSL-Deployments verwendet werden, um Anmeldepaswörter zu verschlüsseln.	Standardmäßig deaktiviert.
Standardzeichensatz	Definiert das Standardzeichen für den Inhalt, der vom/ins Server-Dateisystem heruntergeladen oder hochgeladen wird, oder für die Anzeige von Repository-Dateien in einem Webbrowser. Dieser Wert wird nur verwendet, wenn dem Inhalt, z. B. einer einfachen Textdatei, nicht ausdrücklich ein Zeichensatz zugewiesen wurde.	Ein Wert, der einen Zeichensatz angibt, z. B. UTF-8 oder ASCII.
Leistungsdaten protokollieren	"Wahr" gibt an, dass Leistungsdaten protokolliert werden.	Standardmäßig deaktiviert.
Meldungs-Bus-Benachrichtigung aktiviert	Gibt an, ob der Repository-Server mit dem Meldungs-Bus verknüpft werden soll.	Standardmäßig aktiviert.
Passwortanzeige für Modeler-Parameter	SPSS Modeler-Stream-Parameter, die diesen String enthalten, werden beim Speichern verschlüsselt und in der Benutzeroberfläche maskiert, wenn die Ausführung eines Streams geplant wird.	Maskiertes Passwort.
Größe der Wartenschlange neu indizieren	Definiert die Größe der Warteschlange, die für die Neuindizierung des Repository verwendet wird. Diese Zahl sollte größer sein als der Wert, der in der Konfigurationsoption "Größe des Thread-Pools neu indizieren" definiert wurde.	Ganzzahl. Die Standardeinstellung lautet 15.
Größe des Thread-Pools neu indizieren	Definiert die Zahl der Threads, die für die Neuindizierung des Repository verwendet werden.	Ganzzahl. Die Standardeinstellung lautet 5.
Repository-Wartung aktiviert	Aktiviert bzw. deaktiviert den Wartungsdienst für das Repository.	Wahr oder Falsch. Die Standardeinstellung lautet "Wahr".

Name	Beschreibung	Einstellungen
Wartungshäufigkeit für Repository	Legt die Häufigkeit (in Minuten) fest, mit der der Wartungsdienst für das Repository ausgeführt werden soll. Der Repository-Dienst muss neu gestartet werden, damit die Änderungen wirksam werden.	Ganzzahl. Die Standardeinstellung lautet 60 Minuten.
Repository-Wartung – Master	Legt fest, ob der Wartungsdienst für das Repository nur auf dem Master-Knoten im Server-Cluster ausgeführt werden soll.	Wahr oder Falsch. Die Standardeinstellung lautet "Falsch".
Kontingent für Repository-Wartung	Gibt die Dauer der einzelnen Wartungsintervalle in Minuten an und ermöglicht, dass der Wartungsdienst arbeitet, ohne dass es zu einer übermäßigen Belastung der Systemressourcen und einer übermäßig langen Verarbeitungsdauer bei den Anwendungen kommt. Negative Werte werden als "ohne Begrenzung" interpretiert.	Ganzzahl. Die Standardeinstellung lautet 10 Minuten.
Anfangsdatum für Repository-Wartung	Legt Datum und Uhrzeit für den Start des Wartungsdienstes für das Repository fest. Ungültige Datumsangaben oder Datumsangaben vor dem aktuellen Datum werden ignoriert und der Dienst wird sofort gestartet. Wenn die angegebene Uhrzeit für den Start in der Vergangenheit liegt, wird der Dienst am nächsten Tag zu der angegebenen Uhrzeit gestartet.	Datum und Uhrzeit im Format [JJJ-MM-TT] HH:MM:SS.
Beginn der Repository-Wartung (Max.)	Legt die maximale Verzögerungszeit für den Start des Wartungsdienstes fest.	Ganzzahl. Die Standardeinstellung lautet 30 Minuten.
Beginn der Repository-Wartung (Min.)	Legt die Mindestverzögerungszeit für den Start des Wartungsdienstes fest.	Ganzzahl. Die Standardeinstellung lautet 5 Minuten.
Repository-Benachrichtigung aktiviert	Gibt an, ob der Repository-Server mit dem Benachrichtigungsserver kommunizieren soll.	Standardmäßig deaktiviert.
Ressourcensperre	Aktiviert die Ressourcensperre. Eine Ressourcensperre verhindert, dass eine Ressource gleichzeitig von mehreren Benutzern geändert wird. Wenn aktiviert, kann eine Ressource gesperrt werden und wird für andere Benutzer schreibgeschützt angezeigt.	Standardmäßig aktiviert.
Nachschlagetabelle für Ressourcenübertragung	Zuordnungsimpementierung für ID-Suche beim Übertragen von Ressourcen.	DISK oder MEMORY.

Name	Beschreibung	Einstellungen
Cachegröße für Ressourcenübermittlungs-Seitenergebnis	Größe des Cache für die Speicherung der Seitenergebnisse bei Ressourcenübertragungen. Wenn der Benutzer während der Ressourcenübertragung individuelle Konfliktlösungen ausführt, gibt es möglicherweise mehr Konflikte als auf einmal in der Benutzeroberfläche angezeigt werden können. Die Größe des Ergebnis-Cache bestimmt die Anzahl von Seiten, die für eine einzelne Sitzung zwischengespeichert werden können. Wenn der Benutzer sehr häufig Gebrauch von der individuellen Konfliktlösung macht, könnte eine Vergrößerung des Cache eine Leistungssteigerung herbeiführen; dies führt allerdings auch zu erhöhter Speicherbelastung.	Ganzzahl. Die Standardeinstellung lautet 5.
Aktualisierung der Stream-Eigenschaften	Sofern verfügbar, gibt diese Option an, ob Stream-Eigenschaften aktualisiert werden, wenn die Datei im Repository veröffentlicht wird. Durch Deaktivieren dieser Option (empfohlen) lässt sich eventuell die Leistungsfähigkeit verbessern.	Standardmäßig aktiviert.
Ausführbare Server-Programme validieren	Gibt an, ob ausführbare Server-Programme beim Speichern im Repository validiert werden sollen.	Standardmäßig aktiviert.

Scoring-Service

Mit den Konfigurationsoptionen unter “Scoring-Service” können Sie die Einstellungen für das Scoring festlegen. Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter “Scoring Service” auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-9
Scoring Service-Konfigurationsoptionen

Name	Beschreibung	Einstellungen
Audit-Zeitabstand	Die Zahl der Millisekunden zwischen Audit-Aktualisierungen.	Ganzzahl. Die Standardeinstellung lautet 3600000.

Name	Beschreibung	Einstellungen
Standard-Protokollziel.	Standard-Protokoll-Destination.	Eine deploymentspezifische und/oder serverspezifische Zeichenfolge, bei der Groß- und Kleinschreibung beachtet wird und die vom JNDI-Service verwendet wird, um die JMS-Warteschlange für Scoring-Protokolle zu kennzeichnen.
Maß-Zeitabstand	Die Zahl der Millisekunden zwischen Maß-Aktualisierungen.	Ganzzahl. Die Standardeinstellung lautet 5000.
Hostnamen auflösen	Definiert, ob der Scoring-Service versuchen soll, Hostnamen aufzulösen.	Standardmäßig aktiviert.
Arbeitspool - maximale Größe	Maximale Größe des Arbeiterpools.	Ganzzahl. Die Standardeinstellung lautet 100.

Suchen

Die Suche-Konfigurationsoption ermöglicht es Ihnen, die Anzahl der Treffer, die auf einer Suchergebnisseite in IBM® SPSS® Collaboration and Deployment Services Deployment Manager angezeigt werden sollen, und die Größe des Ergebnis-Sets anzugeben sowie festzulegen, ob Suchen in Audit-Ansichten protokolliert werden sollen. Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter "Suche" auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-10
Konfigurationsoptionen für die Suche

Name	Beschreibung	Einstellungen
Suchvorgang-Audit	Protokolliert jede Suche in der Audit-Ansicht. Für weitere Informationen siehe Thema Auditing des Repository in Kapitel 13 auf S. 116. Beachten Sie, dass das Aktivieren dieser Option die Suchfunktion verlangsamen kann.	Standardmäßig deaktiviert.

Name	Beschreibung	Einstellungen
Standard-Seitengröße	Anzahl der Suchergebnisse, die auf einer Seite angezeigt werden.	Ganzzahl. Die Standardeinstellung lautet 25.
Zeilen maximal	Maximale Anzahl an Zeilen in einem Suchergebnis-Set. Um eine unbegrenzte Anzahl von Ergebnissen anzuzeigen, muss der Wert auf -1 gesetzt werden. Andernfalls muss eine positive Ganzzahl festgelegt werden (um die Größe des ausgegebenen Ergebnis-Sets zu beschränken und Probleme aufgrund von Speicherknappheit und Client-Timeouts zu vermeiden).	Ganzzahl. Die Standardeinstellung lautet -1.

Sicherheit

Die Sicherheitskonfigurationsoptionen ermöglichen es Ihnen, Zugriffseinstellungen für das Repository festzulegen.

Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter "Sicherheit" auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-11
Sicherheitskonfigurationsoptionen

Name	Beschreibung	Einstellungen
Anmeldungen im Cache ablegen	Speichert Anmeldungen für schnellere Reaktion von Webdiensten. Wenn aktiviert, werden Änderungen an Benutzern, Gruppen oder Rollen erst nach 30 Minuten oder später wirksam. Erfordert einen Server-Neustart.	Standardmäßig aktiviert.
Cache-Sitzungs-Zeitüberschreitung	Anzahl der Minuten, bevor die Sicherheitssitzung eines inaktiven Benutzers entfernt wird.	Ganzzahl. Die Standardeinstellung lautet 30.
Intervall für Neuvalidierung der Anmeldung im Cache	Intervall in Minuten für die erneute Überprüfung von Anmeldungen im Cache. Damit Einstellung in Kraft tritt, muss der Server neu gestartet werden.	Ganzzahl. Die Standardeinstellung lautet 5.
Clients deaktivieren	Deaktiviert die Anmeldung für IBM® SPSS® Collaboration and Deployment Services Client-Anwendungen (IBM® SPSS® Collaboration and Deployment Services Deployment Manager, IBM® SPSS® Collaboration and Deployment Services Deployment Portal usw.)	Standardmäßig deaktiviert.

Name	Beschreibung	Einstellungen
Passwort verschlüsseln	Macht die Verwendung verschlüsselter Passwörter für Webdienste erforderlich. Webdienste senden beim Anfordern von Passwörtern einen Verschlüsselungsschlüssel. Der Server verschlüsselt das Passwort mithilfe des bereitgestellten öffentlichen Schlüssels. Wenn Passwort verschlüsseln aktiviert ist, dürfen Webdienste keine Passwörter anfordern, ohne einen Verschlüsselungsschlüssel zu liefern. Dies betrifft Benutzervoreinstellungen, Content-Repository-Anmeldeinformationen und ähnliche Dienste.	Standardmäßig aktiviert.
Benutzer-IDs in Kleinbuchstaben	Erzwingt, dass die interne ID für einen Benutzer in Kleinbuchstaben festgelegt wird. Diese Option sollte nur deaktiviert werden, wenn ein Remote-Benutzerverzeichnis bei Benutzer-IDs zwischen Groß- und Kleinschreibung unterscheidet.	Standardmäßig aktiviert.
Meldung	Die Meldung, die auf dem browserbasierten Begrüßungsbildschirm von IBM® SPSS® Collaboration and Deployment Services Deployment Manager angezeigt wird.	Meldungstext. Zu Formatierungszwecken können HTML-Tags verwendet werden.
Principal normalisieren	Legt fest, dass Benutzernamen in normalisiertem Zeichenformat in der Datenbank gespeichert werden, wenn Benutzer erstellt oder importiert werden (<i>Normalisierungsform C</i> nach dem Unicode-Standard).	Standardmäßig deaktiviert.

Setup

Mit der Konfigurationsoption “Setup” können Sie verschiedene Setupeinstellungen für das Repository festlegen, beispielsweise das auf IBM® SPSS® Collaboration and Deployment Services verweisende URL-Präfix, JMS-Warteschlangeneinstellungen und JMS-Meldungs-Bus-Einstellungen.

Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter “Setup” auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-12
Sicherheitskonfigurationsoptionen

Name	Beschreibung	Einstellungen
Log-JMS Connection Factory	JNDI-Name der Log-JMS Connection Factory.	Eine deploymentspezifische und/oder serverspezifische Zeichenfolge, bei der zwischen Groß- und Kleinschreibung unterschieden wird und die vom JNDI-Service verwendet wird, um die Log-JMS Connection Factory zu kennzeichnen.
Log-JMS-Warteschlange	JNDI-Name der Log-JMS-Warteschlange.	Eine deploymentspezifische und/oder serverspezifische Zeichenfolge, bei der zwischen Groß- und Kleinschreibung beachtet wird und die vom JNDI-Service verwendet wird, um die Log-JMS-Warteschlange zu kennzeichnen.
Meldungs-Bus-JMS Connection Factory	JNDI-Name der Meldungs-Bus-JMS Connection Factory.	Eine deploymentspezifische und/oder serverspezifische Zeichenfolge, bei der zwischen Groß- und Kleinschreibung unterschieden wird und die vom JNDI-Service verwendet wird, um die Meldungs-Bus-JMS Connection Factory zu kennzeichnen.
Meldungs-Bus-JMS-Thema	JNDI-Name des Meldungs-Bus-JMS-Themas.	Eine deploymentspezifische und/oder serverspezifische Zeichenfolge, bei der zwischen Groß- und Kleinschreibung unterschieden wird und die vom JNDI-Service verwendet wird, um das Meldungs-Bus-JMS-Thema zu kennzeichnen.
URL-Präfix	Das Präfix sollte in DNS (oder WINS) aufgelöst werden können. Falls SSL verwendet wird, sollte das Präfix mit <i>https</i> anstelle von <i>http</i> beginnen. Außerdem kann der Port weggelassen werden, wenn der Server den Standard- <i>http</i> -Port 80 oder den Standard- <i>https</i> -Port 443 verwendet. Der Server muss neu gestartet werden, damit Änderungen am Präfix wirksam werden.	URL.

IBM ShowCase

IBM® ShowCase®-Konfigurationsoptionen ermöglichen es Ihnen, die Verbindungseinstellungen anzugeben, die für die Erstellung von IBM® ShowCase® Warehouse Builder-Jobschritten in IBM® SPSS® Collaboration and Deployment Services Deployment Manager verwendet werden.

IBM ShowCase Warehouse Builder wird separat zusammen mit dem IBM ShowCase-Produktset installiert.

Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter IBM ShowCase auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 8-13
IBM ShowCase-Konfigurationsoptionen

Name	Beschreibung	Einstellungen
IBM ShowCase Warehouse Builder-Datenbank	Der Name der Datenbank/Bibliothek für das IBM ShowCase Warehouse Builder-Set und Definitionsinformationen.	Gültiger Datenbank-/Bibliotheksname.
IBM ShowCase Warehouse Builder-Hostname	Die IP-Adresse bzw. der Hostname des IBM i-Servers, der von IBM ShowCase Warehouse Builder verwendet wird.	Eine gültige IP-Adresse bzw. ein gültiger Hostname.
IBM ShowCase Warehouse Builder-Benutzername.	Der Benutzername, der für die Verbindung zu der oben genannten Datenbank/Bibliothek verwendet wird. Dies gilt nur für Installationen des IBM® SPSS® Collaboration and Deployment Services Servers unter Windows.	Benutzername.
IBM ShowCase Warehouse Builder-Benutzerpasswort	Das Passwort, das für die Verbindung zu der oben genannten Datenbank/Bibliothek verwendet wird. Dies gilt nur für Installationen des IBM SPSS Collaboration and Deployment Services Servers unter Windows.	Maskiertes Passwort.

CMOR

Die Option zur CMOR-Konfiguration enthält die Einstellung *Zeichenbeschränkung für UDF*, mit der Sie die maximale Anzahl an Zeichen angeben können, die an benutzerdefinierte Datenbankfunktionen weitergegeben werden können. Der Standardwert ist für die meisten Systeme ausreichend und sollte nur in seltenen Fällen geändert werden müssen. Somit ist die Option "CMOR" in der Standardkonfiguration der Benutzeroberfläche ausgeblendet und ein Zugriff darauf sollte nur erforderlich sein, wenn die Zeichenbeschränkung aufgrund von Fehlern erhöht werden muss. Wenn die Anzahl der in Versionsbezeichnungen verwendeten Zeichen die angegebene Obergrenze überschreitet, kann das System die verfügbare Daten-Provider-Definition – Echtzeit-Liste nur abrufen, wenn ein Daten-Provider für eine Scoring-Konfiguration ausgewählt wird, und das Serverprotokoll enthält Kürzungsfehler. Wenn die Anzahl der Bezeichnungen nicht verringert werden kann, muss die Zeichenbeschränkung für UDF auf einen höheren Wert gesetzt werden. So ändern Sie die Beschränkung:

- Klicken Sie auf der Konfigurationsseite auf die Verknüpfung Konfiguration oben in der Einstellungsliste, um die ausgeblendeten Einstellungen anzuzeigen.

- ▶ Klicken Sie in der Einstellungsliste unter “CMOR” auf Zeichenbeschränkung für UDF. Die aktuelle Obergrenze für die Anzahl der Zeichen wird angezeigt.
- ▶ Ändern Sie den Wert nach Bedarf.
- ▶ Klicken Sie auf Festlegen, um den neuen Wert festzulegen.
- ▶ Melden Sie sich ab und starten Sie den Repository-Server neu.

Bei einigen Datenbanken, wie SQL Server, DB2 oder DB2 auf IBM i, können die Funktionen nicht automatisch mit dem neuen Wert aktualisiert werden. In diesem Fall müssen die Funktionen nach dem Herunterfahren des Servers, jedoch vor seinem Neustart, manuell aktualisiert werden. Gehen Sie dazu wie folgt vor:

- ▶ Stoppen Sie den Server nach der Änderung des Konfigurationswerts.
- ▶ Ändern Sie, nachdem der Server gestoppt wurde, mithilfe der bestehenden Administrationstools für Ihre Datenbank die beiden Funktionen *spsscmor_fn_gl2* und *spsscmor_fn_gl3*. Ersetzen Sie die aktuelle Obergrenze für die Zeichenzahl (ursprünglich 4.000) durch die in der Konfigurationseinstellung *Zeichenbeschränkung für UDF* angegebene Obergrenze.
- ▶ Starten Sie den Server nach dem Aktualisieren der Werte erneut.

In der folgenden Tabelle finden Sie die Ersetzungsangaben für die einzelnen Datenbanken beim Erhöhen der Zeichenbeschränkung von 4.000 auf 6.000.

Tabelle 8-14
Beispiel für die Erhöhung der Zeichenbeschränkung

Datenbank	Alte Spezifikation	Neue Spezifikation
SQL Server	@validLabels nvarchar(4000)	@validLabels nvarchar(6000)
DB2	valid_labels varchar(4000)	valid_labels varchar(6000)
DB2 auf IBM i	valid_labels VARGRAPHIC(4000)	valid_labels VARGRAPHIC(6000)

MIME-Typen

Multipurpose Internet Mail Extensions oder **MIME** ist ein Standard zur Identifizierung von bestimmten Typen von Informationen. Ursprünglich wurde MIME als E-Mail-Erweiterung eingesetzt, es wird aber auch in HTTP-Umgebungen verwendet, um die Inhalte zu definieren, die von einem Server geliefert werden.

Bei der Bearbeitung einer Dateianforderung fügt ein Server der Datei Kopfzeileninformationen hinzu. Zu diesen Informationen gehört der MIME-Typ, der den in der Datei enthaltenen Medientyp angibt. Der Server verwendet die Endung des Dateinamens, um den MIME-Typ zu definieren. Der Client, der die Datei empfängt, verwendet den MIME-Typ, um die beste Methode zur Handhabung der Datei zu bestimmen.

Der Server kontrolliert die Verbindungen zwischen Dateieendungen und MIME-Typen. Um diese Zuordnungen zu konfigurieren, verwenden Sie die IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Seite "MIME-Typen und Dateityp-Symbole", auf die Sie durch Klicken auf MIME-Typen in der Navigationsliste zugreifen können.

Abbildung 9-1
Seite "MIME-Typen und Dateityp-Symbole"

> MIME-Typen und Dateityp-Symbole

:: MIME-Typen und Dateityp-Symbole verwalten

Klicken Sie auf den Namen eines MIME-Typs, um seine Einstellungen zu bearbeiten.

[Neuen MIME-Typ hinzufügen](#)

Name	MIME-Typ	Erweiterungen	Kleines Symbol	Löscher
Analyseplan für komplexe Stichproben	application/vnd.spss-spss-csaplan	csaplan		✗
Analyseplan für komplexe Stichproben	application/vnd.spss-statistics-csaplan	csaplan		✗
Anwendungsansicht	application/vnd.spss-application-view	av		✗
Anwendungsserver-Datenquelle	application/vnd.spss-datasource-appserver			✗
Archive HTML	application/vnd.spss-htmlc	htmlc		✗
Benutzerdef. Dialogpaket	application/vnd.spss-statistics-spd	spd		✗
Benutzervoreinstellung	application/vnd.spss-userPreference			✗
Bitmap-Bild	image/bmp	bmp		✗
Data-Provider-Definition	application/vnd.spss-data-provider	dpd		✗
Daten-Provider-Definition für Zugriff in Echtzeit	application/vnd.spss-data-provider-realtime	dpd-rt		✗
Datenquelle des Datenservice	application/vnd.spss-realtime-dataservice			✗
Domäne	application/vnd.spss-repository-domain	CredentialRealm		✗
Enterprise View	application/vnd.spss-enterprise-view			✗
Erweitertes Windows-Metadateiformat	image/x-emf	emf		✗
Extensible Markup Language-Datei	text/xml	xml		✗
Graphics Interchange Format-Bild	image/gif	gif		✗
Hyper Text Markup Language-Datei	text/html	html htm		✗

Auf der Seite “MIME-Typen und Dateityp-Symbole” können Sie folgende Aufgaben ausführen:

- Hinzufügen von MIME-Typzuordnungen zum Server.
- Bearbeiten vorhandener Einstellungen für MIME-Typen, darunter das Zuweisen von Bildern zu Dateien.
- Löschen von MIME-Typzuordnungen vom Server.

Hinweis: Viele bekannte Symbole werden in IBM® SPSS® Collaboration and Deployment Services Deployment Portal standardmäßig nicht angezeigt. Administratoren können für externe Dateitypen (z. B. *application/msword*) ein Symbol zum MIME-Typ hinzufügen. Für weitere Informationen siehe Thema [Hinzufügen von MIME-Typzuordnungen](#) auf S. 90.

Hinzufügen von MIME-Typzuordnungen

Ein MIME-Typ besteht aus zwei Teilen, einem Typ und einem Untertyp, die durch einen Schrägstrich getrennt sind. Der Typ gibt den allgemeinen Medientyp als *application*, *audio*, *image*, *message*, *model*, *multipart*, *text* oder *video* an. Der Untertyp hingegen kennzeichnet das Format der Medien und variiert je nach Medientyp. *text/html* beispielsweise bezieht sich auf Text im HTML-Format.

Untertypen enthalten häufig Präfixe, um MIME-Typen für spezifische Produkte zu kennzeichnen. Untertypen, die sich auf kommerzielle Produkte beziehen, enthalten zum Beispiel das Präfix *vnd.*, das einen Hersteller-Untertyp angibt, z. B. *application/vnd.ms-access*. Im Gegensatz dazu beinhalten Untertypen für nicht kommerzielle Produkte das Präfix *prs.*, das einen persönlichen Untertyp bezeichnet.

MIME-Typen sollten bei der Internet Assigned Numbers Authority (IANA) registriert sein. Im Fall von Typen, die nicht registriert sind, sollte der Untertyp das Präfix *x-* aufweisen, um einen Konflikt mit Typen zu vermeiden, die unter Umständen zukünftig registriert werden, wie z. B. in *application/x-vnd.spss-clementine-stream*. Eine Liste der registrierten MIME-Typen finden Sie bei der IANA (<http://www.iana.org/assignments/media-types/>).

Hinzufügen einer neue MIME-Typzuordnung:

- ▶ Klicken Sie auf der Seite “MIME-Typen und Dateityp-Symbole” auf Neuen MIME-Typ hinzufügen. Die Seite “MIME-Typen und Dateityp-Symbole hinzufügen” erscheint.

Abbildung 9-2
Erstellung von MIME-Typen

- ▶ Geben Sie einen Namen für den MIME-Typ ein. Der Name dient der Kennzeichnung des Typs, die einfacher zu lesen ist als der Typ selbst. Der Name *Benutzerdefiniertes Dialogfeldpaket* zum Beispiel ist einfacher zu lesen als der Typ *application/x-vnd.spss-statistics-spd*.
- ▶ Geben Sie den hinzuzufügenden MIME-Typ ein.
- ▶ Geben Sie die Dateierweiterungen ein, die mit dem MIME-Typ verbunden werden sollen. Setzen Sie zwischen Einträgen ein Leerzeichen, wenn Sie mehrere Dateierweiterungen angeben.
- ▶ Weisen Sie dem MIME-Typ ein Symbol zu. Dieses Bild sollte 16 x 16 Pixel groß sein und im *.gif*-Format vorliegen. Das Bild wird für gewöhnlich in Inhaltslisten verwendet. Klicken Sie auf *Durchsuchen*, um zu der Datei zu navigieren. Falls kein Symbol zugeordnet werden soll, wählen Sie *Nein*.
- ▶ Klicken Sie auf *Speichern*, um den MIME-Typ hinzuzufügen und zur Seite "MIME-Typen und Dateityp-Symbole hinzufügen" zurückzukehren, oder auf *Abbrechen*, um zurückzukehren, ohne den MIME-Typ auf dem Server zu speichern.

Bearbeiten von MIME-Typzuordnungen

Bearbeitung eines vorhandenen MIME-Typs:

- ▶ Klicken Sie auf der Seite "MIME-Typen und Dateityp-Symbole" auf den Namen des MIME-Typs, der bearbeitet werden soll. Die Seite "MIME-Typen und Dateityp-Symbole bearbeiten" für diesen MIME-Typ wird angezeigt.

Abbildung 9-3
Bearbeiten von MIME-Typen

The screenshot shows a web-based configuration interface for MIME types. The title bar reads '> MIME-Typen und Dateityp-Symbole'. Below it, a sub-header says ':: MIME-Typen und Dateityp-Symbole bearbeiten'. The form contains the following fields and controls:

- Name:** A text input field containing 'HyperText Markup Language-Datei'.
- MIME-Typ:** A text input field containing 'text/html'.
- Erweiterungen:** A text input field containing 'html htm'. Below it, a note reads: 'Trennen Sie bei der Eingabe mehrerer Erweiterungen die einzelnen Erweiterungen durch Leerzeichen.'
- Kleines Symbol:** Two radio buttons, 'Ja' (selected) and 'Nein'. To the right is a search button labeled 'Durchsuchen...'.
- At the bottom right are two buttons: 'Speichern' and 'Abbrechen'.

- ▶ Ändern Sie die Einstellungen wie gewünscht. Symbole werden nur geändert, wenn Sie eine neue Datei oder Nein wählen. Wählen Sie Nein, um ein Symbol zu löschen.
- ▶ Klicken Sie auf Speichern, um die neuen Einstellungen für den MIME-Typ zu speichern und zur Seite "MIME-Typen und Dateityp-Symbole hinzufügen" zu gelangen, oder auf Abbrechen, um zurückzukehren, ohne die MIME-Typ-Einstellungen auf dem Server zu speichern.

Löschen von MIME-Typzuordnungen

Löschen eines vorhandenen MIME-Typs:

- ▶ Klicken Sie auf der Seite "MIME-Typen und Dateityp-Symbole" auf das Löschen-Symbol des MIME-Typs, der gelöscht werden soll.

Die MIME-Typen-Tabelle wird aktualisiert; der gelöschte MIME-Typ ist nicht mehr enthalten.

Neuindizierung des Repository

Die Indizierung wird verwendet, um die IBM® SPSS® Collaboration and Deployment Services Repository-Suche zu optimieren. Standardmäßig wird bei einem Repository-Upgrade der bestehende Index gelöscht und ein neuer Index aufgebaut. Das Repository kann auch so konfiguriert werden, dass die Neuindizierung der Verarbeitungsergebnisse, z. B. eine Job-Ausgabe, beim Start erzwungen wird. Für weitere Informationen siehe Thema [Prozessmanagement](#) in Kapitel 8 auf S. 77. Die Repository-Suche wird automatisch deaktiviert, während die Neuindizierung beim Start läuft.

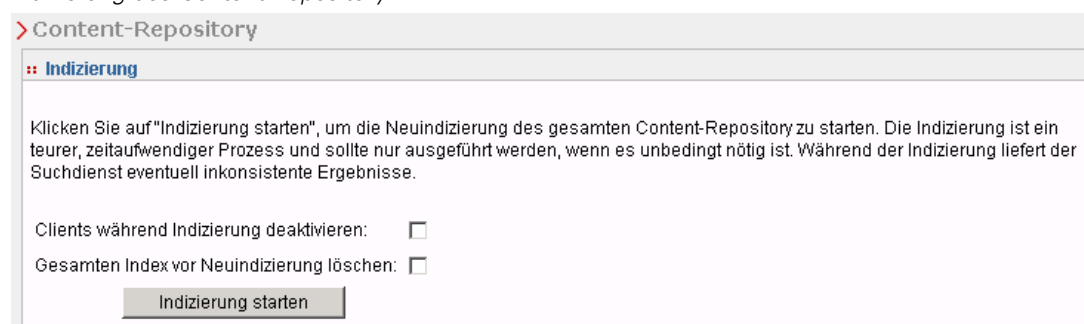
Eine Neuindizierung kann auch im browserbasierten IBM® SPSS® Collaboration and Deployment Services Deployment Manager auf Anforderung eines autorisierten Benutzers durchgeführt werden. Für weitere Informationen siehe Thema [Aktionen](#) in Kapitel 5 auf S. 40.

Hinweis: Die Neuindizierung ist ein ressourcenintensiver und zeitraubender Vorgang, der nur ausgeführt werden sollte, wenn es unbedingt erforderlich ist, z. B. wenn viele neue Daten in das Repository importiert werden. Es wird dringend empfohlen, die Neuindizierung nur dann auszuführen, wenn in IBM® SPSS® Collaboration and Deployment Services keine Benutzeraktivität stattfindet. Wenn sichergestellt werden kann, dass alle Benutzer während der Neuindizierung abgemeldet sind, muss die Repository-Suche deaktiviert werden. Es ist jedoch nicht ratsam, den Index zu löschen, während das System benutzt wird.

So indizieren Sie das Repository neu:

1. Klicken Sie im browserbasierten Deployment Manager in der Navigationsliste auf Repository-Index. Die Seite "Indizierung des Content-Repository" wird geöffnet.

Abbildung 10-1
Indizierung des Content-Repository



2. Führen Sie eine der folgenden Aktionen aus:
 - Wenn keine Benutzer beim Repository angemeldet sind, wählen Sie Gesamten Index vor Neuindizierung löschen.
 - Wenn noch Benutzer beim Repository angemeldet sind, wählen Sie Clients während Indizierung deaktivieren.
3. Klicken Sie auf Indizierung starten. Während der Index neu erstellt wird, zeigt die Seite "Indizierungsstatus des Content-Repository" die Statistik der verarbeiteten Objekte.

Abbildung 10-2*Indizierungsstatus des Content-Repository*

> Content-Repository	
:: Indizierungsstatus	
Status:	In Arbeit
Suche deaktiviert:	Nein
Index löschen:	Ja
Fehleranzahl:	0
Letzter Fehler:	
Anfangszeit:	Feb 2 2010 5:27:14 AM
Verstrichene Zeit:	00:00:00 (hh:mm:ss)
Thread-Poolgröße:	0
Warteschlangengröße:	0
Anzahl an wartenden Elementen:	0
Indizierte Ordner:	0
Indizierte Themen:	0
Indizierte Dateien:	0
Geschwindigkeit:	□ Objekte/Sekunde

Benachrichtigungen

IBM® SPSS® Collaboration and Deployment Services bietet die Mechanismen von **Benachrichtigungen** und **Abonnements**, um die Benutzer über Änderungen an IBM® SPSS® Collaboration and Deployment Services Repository-Objekten und Jobverarbeitungsergebnisse auf dem Laufenden zu halten. Sowohl Benachrichtigungen als auch Abonnements erzeugen E-Mail-Meldungen, wenn entsprechende Ereignisse eintreten. Wenn beispielsweise ein Job fehlschlägt, kann IBM SPSS Collaboration and Deployment Services automatisch eine E-Mail an die für den Job verantwortliche Person senden. Der Fehler löst eine Suche nach einer Vorlage aus, die dem Ereignis entspricht. Durch Anwenden der Vorlage auf das Ereignis wird eine E-Mail erzeugt, die an alle mit dem Ereignis verbundenen Empfänger gesendet wird.

Benachrichtigungsvorlagen, die in der Repository-Standardinstallation inbegriffen sind, befinden sich in Unterverzeichnissen von `<Installationsverzeichnis>\components\notification\templates`. Die Namen der Unterverzeichnisse entsprechen dem allgemeinen Ereignistyp. Beispielsweise enthält der Ordner `components\notification\templates\PRMS\Completion` zwei Meldungsvorlagen. Diese Vorlagen, `job_success.xml` und `job_failure.xml`, entsprechen der erfolgreichen (success) bzw. fehlgeschlagenen (failure) Jobausführung. Wenn ein Job erfolgreich abgeschlossen wird, verwendet IBM SPSS Collaboration and Deployment Services die Vorlage `job_success`, um eine Benachrichtigungsmeldung zu generieren, die die erfolgreiche Ausführung mitteilt. Inhalt und Erscheinungsbild der Benachrichtigungsmeldungen können durch Ändern der Vorlagen angepasst werden.

Struktur von Benachrichtigungsmeldungsvorlagen

Benachrichtigungsvorlagen wandeln Ereignisinformationen in Benachrichtigungsmeldungen um und verwenden dafür Apache **Velocity** Template Language.

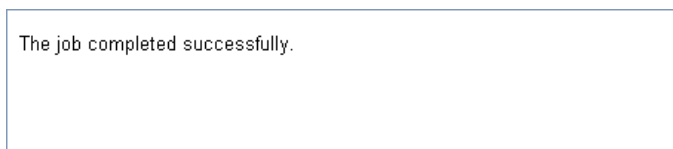
Struktur von Velocity-Vorlagen

Eine Velocity-Vorlage hat die Dateiendung `*.vm`. Die Vorlage generiert eine Meldung anhand des Operators `"="`, um die Werte `/mimeMessage/messageSubject`, `/mimeMessage/messageContent` und `/mimeMessage/messageProperty` zuzuordnen, die daraufhin vom E-Mail-Prozessor analysiert werden. Über die folgende Beispielvorlage wird eine einfache, generische E-Mail-Nachricht generiert, die den Erfolg des entsprechenden Jobs meldet.

```
/mimeMessage/messageSubject=Job Completion  
/mimeMessage/messageContent[text/plain;charset=utf-8]=The job completed successfully.
```

Die daraus resultierende E-Mail ist in folgender Abbildung dargestellt.

Abbildung 11-1
Generische Benachrichtigungsmeldung



Weitere Informationen zu Velocity finden Sie in der Dokumentation des Apache [Velocity Project](http://velocity.apache.org/) (<http://velocity.apache.org/>).

Meldungseigenschaften

E-Mail-Benachrichtigungsvorlagen können Eigenschaften enthalten, die festlegen, wie eine Meldung verarbeitet werden soll, wenn die SMTP-Einstellungen von den zu verwendenden Repository-Standards abweichen. Zum Beispiel könnte es notwendig sein, einen abweichenden SMTP-Servernamen und eine abweichende SMTP-Portnummer oder die Antwort-E-Mail-Adresse anzugeben, die der Nachricht zugeordnet ist. Die Standard-SMTP-Eigenschaften sind unter den Repository-Konfigurationsoptionen für Benachrichtigungen aufgeführt. Für weitere Informationen siehe Thema [Benachrichtigung](#) in Kapitel 8 auf S. 70. Falls Sun JVM zusammen mit der Repository-Installation verwendet wird, entsprechen die SMTP-Eigenschaften den Java Mail API-Eigenschaften für den Umgang mit Nachrichten. definiert in der [folgenden Tabelle](#). Beachten Sie, dass diese Eigenschaften unter Umständen in unterschiedlichen Java-Umgebungen voneinander abweichen. Detaillierte Informationen zu SMTP-Eigenschaften finden Sie in der JVM-Herstellerdokumentation.

Tabelle 11-1
Meldungseigenschaften

Meldungseigenschaft	Attribut	Ereigniseigenschaft	Beschreibung
mail.debug	Wert	MailSmtpDebug	Ein Boole'scher Wert, der den anfänglichen Debug-Modus angibt. Der Standardwert lautet "falsch".
mail.smtp.user	Wert	MailSmtpUser	Der Standard-SMTP-Benutzername.
mail.smtp.password	Wert	MailSmtpPassword	Das SMTP-Benutzerpasswort.
mail.smtp.host	Wert	MailSmtpHost	Der SMTP-Server, mit dem eine Verbindung hergestellt werden soll.
mail.smtp.port	Wert	MailSmtpPort	Der Port des SMTP-Servers, über den eine Verbindung hergestellt werden soll. Der Standardwert lautet "25".
mail.smtp.connectiontimeout	Wert	MailSmtpConnectionTimeout	Der Zeitbeschränkungswert für die Socket-Verbindung in Millisekunden. Der Standardwert für die Zeitbeschränkung lautet "unendlich".
	Wert	MailSmtpTimeout	Der Zeitbeschränkungswert für Socket-E/A in Millisekunden. Der Standardwert für die Zeitbeschränkung lautet "unendlich".

Meldungseigenschaft	Attribut	Ereigniseigenschaft	Beschreibung
mail.smtp.from	Wert	MailSmtFrom	Die E-Mail-Adresse, die für den Befehl SMTP MAIL verwendet wird. Dadurch wird die Umschlagadresse eingestellt.
mail.smtp.from	Label	MailSmtFromPersonal	Das Umschlagadress-Label
mail.smtp.localhost	Wert	MailSmtLocalhost	Der Name des lokalen Hosts. Diese Eigenschaft muss normalerweise nicht eingestellt werden, wenn Ihr JDK und Ihr Name-Service korrekt konfiguriert sind.
mail.smtp.ehlo	Wert	MailSmtEhlo	Ein Boole'scher Wert, der angibt, ob die Anmeldung über den EHLO-Befehl durchgeführt werden soll oder nicht. Standard ist wahr. Für gewöhnlich wird bei einem Versagen des EHLO-Befehls auf den HELO-Befehl zurückgegriffen. Diese Eigenschaft sollte nur für Server verwendet werden, bei denen kein solcher Rückgriff erfolgt.
mail.smtp.auth	Wert	MailSmtAuth	Ein Boole'scher Wert, der angibt, ob der Benutzer über den AUTH-Befehl authentifiziert werden soll oder nicht. Der Standardwert lautet "falsch".
mail.smtp.dsn.notify	Wert	MailSmtDsnNotify	Gibt die Umstände an, unter denen der SMTP-Server Benachrichtigungen über den Zustellungsstatus an den Absender der Meldung senden soll. Gültige Werte sind: <ul style="list-style-type: none"> ■ NEVER gibt an, dass keine Benachrichtigung gesendet werden soll. ■ SUCCESS gibt an, dass nur bei einer erfolgreichen Zustellung eine Benachrichtigung gesendet werden soll. ■ FAILURE gibt an, dass nur bei einer fehlgeschlagenen Zustellung eine Benachrichtigung gesendet werden soll. ■ DELAY gibt an, dass eine Benachrichtigung nur gesendet werden soll, wenn die Meldung verzögert ist. Wenn mehrere Werte angegeben werden, wird ein Komma als Trennzeichen verwendet.

Die Syntax für die Definition dieser Eigenschaften in einer Velocity-Vorlage lautet:

- Der Eigenschaftswert muss `mimeMessage/messageProperty` zugeordnet werden, wobei der Eigenschaftsname und die Bezeichnungsargumente in eckigen Klammern stehen müssen, wie im folgenden Beispiel angegeben:

```
/mimeMessage/messageProperty[smtp.mail.smtp.from][Brian McGee]=bmagee@mycompany.com
```

- Der Wert der Eigenschaftsbezeichnung ist optional, sodass folgende Syntax bei Zuordnungsanweisungen möglich ist:

```
/mimeMessage/messageProperty[smtp.mail.smtp.from][]=bmagee@mycompany.com
```

- Die Werte für Eigenschaftsname und -bezeichnung können als statische Werte oder durch Variablen angegeben werden, die die entsprechenden Ereignisseigenschaften referenzieren:

```
/mimeMessage/messageProperty[smtp.mail.smtp.from][$MailSmtpFromPersonal]=$MailSmtpFrom
```

Meldungsinhalt

Der Inhalt einer Benachrichtigungsmeldung entspricht dem Text, der für die Elemente `messageSubject` und `messageContent` der Benachrichtigungsvorlage angegeben wird. Für beide Elemente kann dieser Text variable Ereignisseigenschaftswerte enthalten.

- In Velocity-Vorlagen werden variable Werte mittels der `$`-Notation referenziert. `Job step ${JobName}/${JobStepName} failed at ${JobStepEnd}` zum Beispiel fügt den Text mit den aktuellen Werten für die Eigenschaften `JobName`, `JobStepName` und `JobStepEnd` ein.

Die Variablen, die in eine Meldung eingefügt werden können, referenzieren die Eigenschaften des Ereignisses, das die Benachrichtigung auslöst. Zu den typischen Eigenschaften gehören:

- `JobName`, eine Zeichenfolge, die den Namen des Jobs angibt.
- `JobStart`, ein Zeitstempel, der die Beginnzeit des Jobs angibt.
- `JobEnd`, ein Zeitstempel, der die Endzeit des Jobs angibt.
- `JobSuccess`, ein Boole'scher Wert, der anzeigt, ob der Job erfolgreich war oder nicht.
- `JobStatusURL`, eine Zeichenkette, die den URL angibt, über den der Job-Status aufgerufen werden kann.
- `JobStepName`, eine Zeichenfolge, die den Namen des Jobs angibt.
- `JobStepEnd`, ein Zeitstempel, der die Endzeit des Jobs angibt.
- `JobStepArtifacts`, ein Array von Zeichenkettenwerten, das die URLs der Ausgabedateien für Jobschritte angibt.
- `JobStepStatusURL`, eine Zeichenkette, die den URL angibt, über den der Jobschritt-Status aufgerufen werden kann.
- `ResourceName`, eine Zeichenfolge, die den Namen des Objekts angibt, das von dem Ereignis betroffen ist, z. B. den Datei- oder Ordnernamen.
- `ResourcePath`, eine Zeichenfolge, die den Pfad des Objekts angibt, das von dem Ereignis betroffen ist.

- *ResourceHttpUrl*, eine Zeichenfolge, die den HTTP-URL angibt, unter dem das Objekt gefunden werden kann.
- *ChildName*, eine Zeichenfolge, die den Namen des untergeordneten Objekts des übergeordneten Objekts angibt, das von dem Ereignis betroffen ist. Wenn beispielsweise eine Datei in einem Ordner erstellt wird, ist dies der Name der Datei.
- *ChildHttpUrl*, eine Zeichenfolge, die den HTTP-URL angibt, unter dem das untergeordnete Objekt gefunden werden kann.
- *ActionType*: für Repository-Ereignisse ist dies der Aktionstyp, der das Ereignis herbeiführte—z. B. FolderCreated.

Die verfügbaren Eigenschaften werden durch das Ereignis definiert und sind je nach Ereignistyp unterschiedlich..

Über die folgende Beispiel-Velocity-Vorlage für Benachrichtigungen beim Erfolg von Jobschritten werden die Namen des Jobs und des Jobschritts in die Betreffszeile eingefügt. Der Inhalt der Meldung enthält außerdem die Endzeiten für den Schritt, den URL, über den der Status aufgerufen werden kann, sowie eine Liste von Artefakten, die durch den Jobschritt generiert wurden. Beachten Sie, dass die Vorlage die `#foreach`-Schleifenstruktur verwendet, um die URLs der Artefakte aus dem *JobStepArtifacts*-Eigenschafts-Array abzurufen.

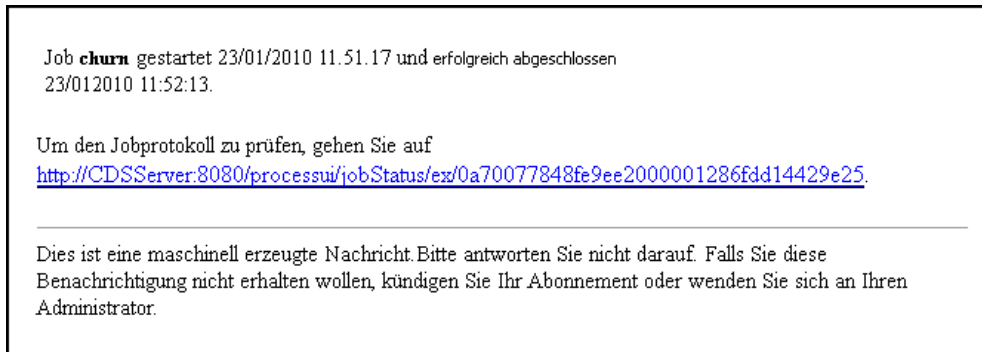
```
<html>
<head>
<meta http-equiv='Content-Type' content='text/html;charset=utf-8'/>
</head>
<body>
<p>Der Job <b>${JobName}</b> wurde am ${JobStart} gestartet und #if(${JobSuccess}) erfolgreich abgeschlossen
#else ist fehlgeschlagen #end ${JobEnd}.

<p>Um das Job-Protokoll zu prüfen, gehen Sie auf <a href='${JobStatusURL}'>${JobStatusURL}</a>.</p>

<hr><p>Dies ist eine maschinell erzeugte Nachricht. Bitte antworten Sie nicht darauf. Wenn Sie diese Benachrichtigung nicht
erhalten möchten, tragen Sie sich aus der Benachrichtigungsliste aus oder wenden sich an Ihren Repository-Administrator.</p>
</body>
</html>
```

Die daraus resultierende E-Mail ist in folgender Abbildung dargestellt.

Abbildung 11-2
Meldung unter Verwendung von angepasstem Inhalt



Die folgenden Code-Abschnitte zeigen, wie die Velocity-Vorlage für Benachrichtigungen über Ordnerinhalte verändert werden kann, um den Hyperlink auf den Job aus der Meldung zu entfernen. IBM® SPSS® Collaboration and Deployment Services-Jobs können nicht außerhalb von IBM® SPSS® Collaboration and Deployment Services Deployment Manager geöffnet werden; aus diesem Grund wird dringend empfohlen, die Benachrichtigungsmeldung so zu ändern, dass der Hyperlink entfernt wird. Die zusätzliche Wenn-Bedingung im Beispiel prüft den MIME-Typ des Objekts; wenn das Objekt ein IBM SPSS Collaboration and Deployment Services-Job ist, wird der Hyperlink nicht eingefügt.

Ursprüngliche Vorlage:

```
#if($Attachments)
Siehe Anhang.
#else
<p>Um den Inhalt der Datei zu prüfen, gehen Sie auf <a href='${ResourceHttpUrl}'>${ResourceHttpUrl}</a>.</p>
#end
```

Geänderte Vorlage:

```
#if($Attachments)
Siehe Anhang.
#else
#if($MimeType!='application/x-vnd.spss-prms-job')
<p>Um den Inhalt der Datei zu prüfen, gehen Sie auf <a href='${ResourceHttpUrl}'>${ResourceHttpUrl}</a>.</p>
#end
#end
```

Meldungsformat

Eine Benachrichtigungsvorlage muss den MIME-Typ des Meldungsinhalts angeben. In Benachrichtigungsvorlagen ist das MIME-Typ-Argument in eckigen Klammern mit `/mimeMessage/messageContent` angegeben.

Der MIME-Typ kann einen von zwei Werten annehmen:

- *text/plain*. Benachrichtigungsmeldungen erscheinen als Standardtext. Dies ist die Standardeinstellung.
- *text/html*. Benachrichtigungsmeldungen enthalten HTML-Tags. Verwenden Sie diese Einstellung, um das Erscheinungsbild des Inhalts in der Meldung zu beeinflussen. Die HTML-Tags in der Meldung müssen einwandfrei gebildet werden.

Es ist sinnvoll, die Vorlagenausgabe immer als Unicode (UTF-8) zu kodieren.

HTML-Benachrichtigungsvorlagen können die Funktionen nutzen, die im Markup erlaubt sind. Zum Beispiel kann die Meldung einen Link auf eine Webseite oder zu einer Job-Ausgabe enthalten.

Folgende Vorlage generiert eine Benachrichtigungsmeldung für den Abschluss von Jobschritten, formatiert den Inhalt als Tabelle, gibt die Hintergrundfarbe für die Nachricht mithilfe eines Inline-Stils für den Nachrichtenkörper an und definiert mithilfe eines internen Stylesheets einen blauen Verdana-Zeichensatz für Textabsätze. Die Nachricht enthält außerdem einen Link auf die Job-Ausgabe.

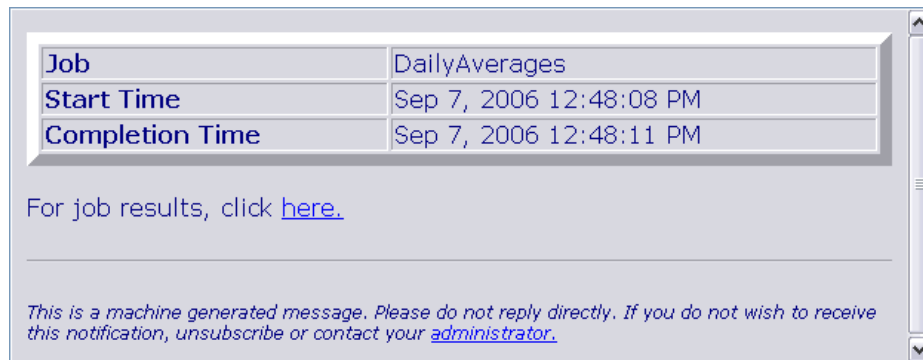
```
/mimeMessage/messageSubject=${JobName}/${JobStepName} completed successfully
/mimeMessage/messageContent[text/html;charset=utf-8]=
```

```
<html>
<head>
<meta http-equiv=Content-Type content=text/html;charset=utf-8/>
<style type=text/css>
table {font-family: verdana; color: #000080}
p {font-family: verdana; color: #000080}
.foot {font-size: 75%; font-style: italic} </style>
</head>
<body style=background-color: #DCDCDC>
<table border=8 align=center width = 100%>
<tr align=left>
<th>Job/step name</th>
<td>${JobName}/${JobStepName}</td>
</tr>
<tr align=left>
<th>End time</th>
<td> ${JobStepEnd}</td>
</tr>
<tr align=left>
<th>Output</th>
<td><p>
#if ($JobStepArtifacts)
#foreach($artifact in $JobStepArtifacts)
  <a href=' $artifact.get(url)'>$artifact.get(filename)</a><br>
#end
#else None <br>
#end
<p></td>
</tr>
</table>
<hr/>
```

```
<p class=foot>This is a machine generated message.
Please do not reply directly. Falls Sie diese Benachrichtigung
nicht erhalten wollen, kündigen Sie Ihr Abonnement oder wenden Sie sich an Ihren
<a href=mailto:admin@mycompany.com> IBM SPSS Deployment
Services-Administrator.</a></p></body>
</html>
```

Die daraus resultierende E-Mail ist in folgender Abbildung dargestellt.

Abbildung 11-3
Meldung unter Verwendung von angepasster Formatierung



Bearbeiten von Benachrichtigungsvorlagen

So bearbeiten Sie eine Velocity-Benachrichtigungsvorlage:

1. Öffnen Sie die Vorlage in einem Texteditor. Unterordner des Ordners *components/notification/templates* enthalten das aktuell verwendete Vorlagen-Set.
2. Ändern Sie den Wert, der */mimeMessage/messageSubject* zugeordnet ist. Verwenden Sie die $\$$ -Notation, um Ereignisseigenschaftsvariablen in das Benachrichtigungsthema einzufügen. Für weitere Informationen siehe Thema [Meldungsinhalt](#) auf S. 98.
3. Definieren Sie den MIME-Typ der Meldung. Der Wert des MIME-Typs wird in den eckigen Klammern hinter *messageContent* angegeben. Verwenden Sie für eine Standardtextmeldung den Wert *text/plain*. Verwenden Sie für eine HTML-Meldung den Wert *text/html*. Für weitere Informationen siehe Thema [Meldungsformat](#) auf S. 100.
4. Ändern Sie den Wert, der *messageContent* zugeordnet ist. Verwenden Sie die $\$$ -Notation, um Ereignisseigenschaftsvariablen in den Inhalt der Meldung einzufügen.
5. Speichern Sie die Vorlage unter Verwendung ihres ursprünglichen Namens.

Daraufhin werden für Benachrichtigungsmeldungen die modifizierten Vorlagen verwendet, wenn das entsprechende Ereignis eintritt.

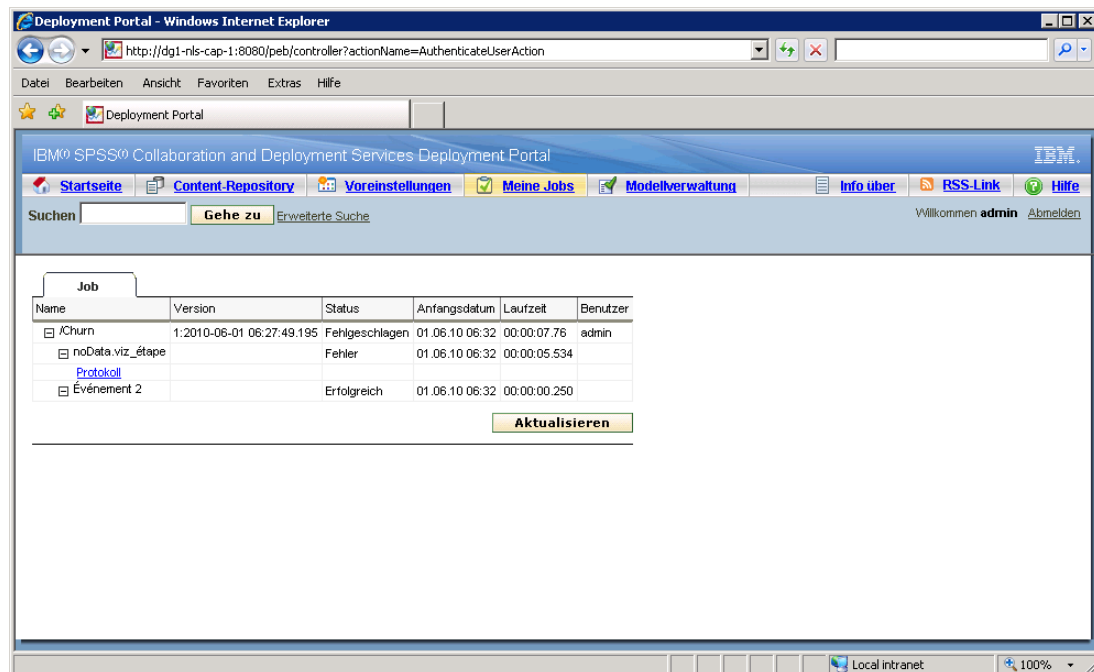
Jobstatus

Eine Benachrichtigungsvorlage, die die Eigenschaft *JobStatusURL* enthält, ergibt eine Meldung mit einem Link zu Job-Ausgabe und -Protokoll.

So zeigen Sie die Ergebnisse eines Jobs an:

1. Klicken Sie auf den Status-Link in der Benachrichtigungsmeldung. Die Anmeldungsseite für den Server wird geöffnet.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein. Klicken Sie auf Anmelden. Die Seite "Jobstatus" wird geöffnet.

Abbildung 11-4
Jobstatus



In der Anzeige des Jobstatus wird der Verarbeitungsstatus eines Jobs inklusive der Informationen zum Status aller Jobschritte im Job angezeigt. Über diese Ansicht können Sie das Jobprotokoll, die Protokolle einzelner Jobschritte und die erzeugte Ausgabe anzeigen.

Jobdetails

Name. Der Repository-Pfad des Jobs.

Version. Die Versionsbezeichnung des Jobs.

Status. Der Verarbeitungsstatus eines Jobs, beispielsweise *In Verarbeitung*, *Abgeschlossen* oder *Fehlgeschlagen*.

Anfangsdatum. Datum und Uhrzeit des Beginns der Jobverarbeitung.

Laufzeit. Die Dauer der Jobausführung.

Benutzer. Der Benutzer, von dem der Job übergeben wurde.

- ▶ Um den Status des Jobs zu aktualisieren, klicken Sie auf Aktualisieren.
- ▶ Um die Details für den Job zu erweitern, die das Jobprotokoll und die Jobschritte enthalten, klicken Sie auf + neben dem Jobnamen.
- ▶ Um das Jobprotokoll anzuzeigen, klicken Sie auf den Link Protokoll unter dem Jobnamen. Die Registerkarte "Protokoll" wird geöffnet. Um die Registerkarte zu schließen, klicken Sie auf Schließen.

Details zu Jobschritten

Name. Der Name des Jobschritts.

Status. Der Verarbeitungsstatus eines Jobschritts, beispielsweise *In Verarbeitung*, *Abgeschlossen* oder *Fehlgeschlagen*.

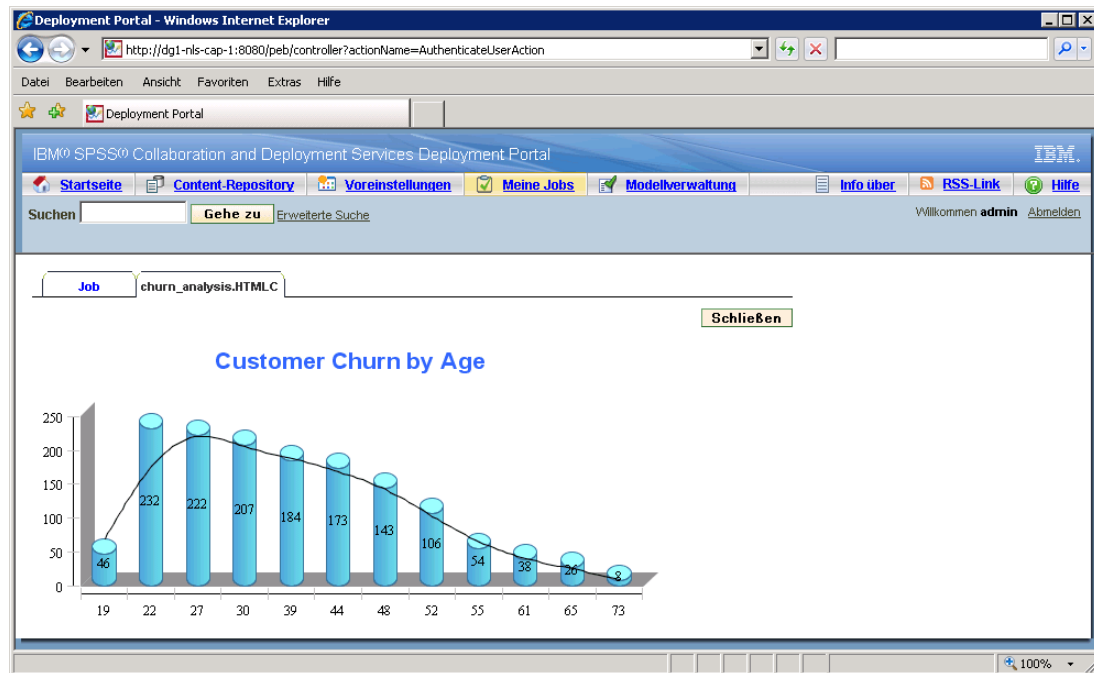
Anfangsdatum. Datum und Uhrzeit des Beginns der Jobschrittverarbeitung.

Laufzeit. Die Dauer der Jobschrittausführung.

- ▶ Um die Details für den Jobschritt zu erweitern, die das Jobschrittprotokoll und alle resultierenden Ausgaben enthalten, klicken Sie auf das + neben dem Jobschrittnamen.
- ▶ Um das Jobschrittprotokoll anzuzeigen, klicken Sie auf den Link Protokoll unter dem Jobschrittnamen. Das Protokoll für den Jobschritt wird in einer neuen Registerkarte geöffnet. Um die Registerkarte zu schließen, klicken Sie auf Schließen.
- ▶ Um das Ergebnis des Jobschritts anzuzeigen, klicken Sie auf den Namen der Ausgabedatei. Die Registerkarte "Ergebnisse" wird geöffnet. Um die Registerkarte zu schließen, klicken Sie auf Schließen.

Der hier gezeigte Beispiel-Job besteht aus drei Schritten. Der erste Schritt umfasst die Datenvorbereitung, die zweite einen BIRT-Bericht und die dritte die Bereinigung der temporären Dateien.

Abbildung 11-5
Job-Ausgabe



Optimieren der Leistung des Benachrichtigungsdienstes

Die Gesamtleistung des Benachrichtigungsdienstes ist eine Kombination aus der Leistung von IBM® SPSS® Collaboration and Deployment Services-Komponenten, die Abonnenten- und Abonnementdaten verwalten, Ereignisse erfassen sowie Benachrichtigungen generieren, formatieren und verteilen, und der Leistung des Datenbanksystems, das die Abonnementdaten speichert und verarbeitet. Benachrichtigungsfunktionen von IBM SPSS Collaboration and Deployment Services erfordern erhebliche Systemressourcen und benötigen eventuell eine Feineinstellung. Es wird auch empfohlen, die allgemeinen Richtlinien zur Verbesserung der Leistung des Benachrichtigungsdienstes zu befolgen.

Konfiguration des Benachrichtigungsdienstes

Konfigurationsoptionen für Benachrichtigungen

Die Leistung des Benachrichtigungsdienstes kann durch Ändern der Parameter erzielt werden, die durch die Konfigurationsoptionen für Benachrichtigungen definiert sind. Die folgenden Optionen können die Leistung spürbar positiv beeinflussen:

- Die Filterung von Ereignissen ermöglicht dem System, Benachrichtigungsereignisse zu ignorieren, für die keine entsprechenden Abonnements oder verknüpfte Benachrichtigungs-Provider im Prozess vorhanden sind. Die Cachegröße des Ereignisfilters definiert die maximale Anzahl an Ereignissen, die im Cache abgelegt werden und für die keine entsprechenden Abonnements vorhanden sind. Das Aktivieren des Ereignisfilters

(Konfigurationsoption *Ereignisfilter*) und ggf. die zusätzliche Vergrößerung des Cache (Konfigurationsoption *Ereignisfilter-Cache*) kann die Leistung des Benachrichtigungsdienstes verbessern. Vom Deaktivieren des Ereignisfilters in Produktionsumgebungen wird abgeraten; dies sollte nur zu Debug- und Testzwecken erfolgen.

- Der Abonnement-ID-Cache ist ein Cache mit Zuordnungen für die aufgelösten Filterausdrücke zur Liste der entsprechenden Abonnement-IDs. Die Größe des Cache definiert die Anzahl der Filterausdrücke im Cache. Zwar gibt es keine Beschränkung bei der Anzahl der entsprechenden Abonnement-IDs, die mit den Filterausdrücken verknüpft sind, jedoch wird erwartet, dass die Anzahl der entsprechenden Abonnements pro aufgelösten Filterausdruck relativ klein ist - etwa einige Dutzend oder in wenigen Fällen mehrere Hundert. Vergrößern des Cache (Konfigurationsoption *Abonnement-ID-Cache*) kann die Leistung verbessern.
- Die persistente Ereigniswarteschlange ermöglicht dem System, einen Cache der eingehenden Benachrichtigungsereignisse im temporären Plattenspeicher zu führen, um den Umfang des verbrauchten Speichers zu minimieren. Standardmäßig werden eingehende Benachrichtigungsereignisse im Arbeitsspeicher aufbewahrt. Wenn die Rate der eingehenden Ereignisse hoch ist und der verfügbare RAM nicht ausreicht, ist es möglich, Ereignisse im temporären Speicherbereich des Datenträgers zu speichern. Wenn die persistente Ereigniswarteschlange aktiviert ist, legt die Festschreibungs-Batchgröße für Ereigniswarteschlangenspeicher die maximale Anzahl an Benachrichtigungsereignissen fest, die im Arbeitsspeicher aufbewahrt wird, bevor sie in den temporären Speicher ausgelagert wird. Zwar können die aktivierte persistente Ereigniswarteschlange (Konfigurationsoption *Persistente Ereigniswarteschlange aktiviert*) und eine größere Festschreibungs-Batchgröße (Konfigurationsoption *Größe der persistenten Ereigniswarteschlange*) die Leistung verbessern, jedoch werden wegen der zusätzlichen Speicheranforderungen nur moderate Erhöhungen der Batch-Größe empfohlen. Das Vergrößern der Speicherdatei der persistenten Ereigniswarteschlange auf dem Datenträger (Option *Größe der persistenten Ereigniswarteschlange*) hat keinen spürbaren Einfluss auf die Leistung. Beachten Sie, dass das System neu gestartet werden muss, damit die Änderungen an der persistenten Warteschlange wirksam werden.
- Durch Deaktivieren von binären Inhalten (E-Mail-Anhänge), die mit der Benachrichtigungsmeldung gesendet werden, kann die Leistung signifikant verbessert werden (Konfigurationsoption *Binärer Inhalt aktiviert*). Das Generieren der Benachrichtigungsmeldungen mit binären Anhängen kann ein verarbeitungsintensiver Vorgang sein. Der Inhalt des binären Anhangs muss aus dem Repository gelesen, an die Benachrichtigungsmeldung angehängt und durch den geeigneten Distributionskanal, z. B. einen E-Mail-Server, geleitet werden. Auch kann eine Transformation des binären Inhalts des Anhangs für bestimmte Arten von Benachrichtigungsmeldungen erforderlich sein. Beispielsweise vergrößern binäre Anhänge mit Base64-Kodierung (SMTP) die Gesamtgröße der generierten Meldungen um etwa 33 %. Die Verarbeitung des Overheads kann sogar noch umfangreicher werden, wenn eine Reihe von verschiedenen benutzerdefinierten Vorlagen zur Formatierung von Benachrichtigungsmeldungen mit umfangreichen Anhängen verwendet wird. In diesen Fällen muss der Benachrichtigungsdienst Meldungen formatieren, Anhänge hinzufügen und jede Meldung separat durch den Distributionskanal "pushen". Für eine verbesserte Leistung ist es ratsam, die Anzahl der Benachrichtigungen mit Anhängen, die

Größe der Anhänge und die Anzahl der benutzerdefinierten Vorlagen zur Formatierung von Benachrichtigungsmeldungen mit Anlagen zu begrenzen.

- Die Verarbeitung und Verteilung von Benachrichtigungsmeldungen ist äußerst ressourcenintensiv. Für kleinere Installationen, oder wenn IBM® SPSS® Collaboration and Deployment Services nicht auf einem dedizierten Server installiert ist, empfiehlt es sich, die Größe des Pools auf einen einzelnen Hintergrund-Thread zu begrenzen, indem Sie die Konfigurationsoptionen *Größe des Sammlungspools für Core-Ereignisse* und *Maximale Größe des Sammlungspools für Core-Ereignisse* ändern.

Eine vollständige Liste der Konfigurationsoptionen, ausführliche Beschreibungen und Standardwerte finden Sie unter [Benachrichtigung auf S. 70](#)

Dedizierter SMTP-Server

Die Leistung des Zustellungskanal, z. B. eines E-Mail-Servers, ist der entscheidende Faktor bei der Steuerung der Gesamtleistung des Benachrichtigungsdienstes. Für IBM SPSS Collaboration and Deployment Services-Benachrichtigungen wird dringend der Einsatz eines schnellen, dedizierten SMTP-Servers anstelle des regulären E-Mail-Servers des Unternehmens empfohlen. Es wurde gezeigt, dass der Einsatz eines dedizierten Servers die erforderliche Zeit für das Hinzufügen einer Benachrichtigungsmeldung in die Mailer-Warteschlange erheblich verkürzt und damit die Leistung des Benachrichtigungsdienstes deutlich verbessert. Eine mögliche Konfiguration besteht im Einsatz eines dedizierten E-Mail-Servers auf demselben Host wie das Repository, was die erforderliche Zeit verkürzt, die der Benachrichtigungsdienst zur Kommunikation mit dem E-Mail-Server über das Netzwerk benötigt.

Anzahl der Threads

Es ist entscheidend, dass die Anzahl der Threads, die vom SMTP-Server zugewiesen werden, ausreichend ist. Die Anzahl muss größer oder gleich der Anzahl der Verarbeitungs-Threads im Ereignissammlungspool des IBM SPSS Collaboration and Deployment Services-Benachrichtigungsdienstes sein. Wenn die Anzahl an Threads auf dem Distributionsserver nicht ausreicht, kann der Benachrichtigungsdienst nicht effizient mit diesem kommunizieren.

Allgemeine Empfehlungen

Mithilfe der folgenden Techniken lässt sich die Leistung des Benachrichtigungsdienstes deutlich verbessern, ohne die verfügbare IBM® SPSS® Collaboration and Deployment Services-Gesamtfunktionalität für den Benutzer zu verringern.

Minimieren der Empfängeranzahl.

Zur Minimierung der Gesamtzeit für Empfängerzusammenstellung beim Ereignisabgleich ist es ratsam, ein Set an externen Verteilerlisten zu definieren, anstatt jeden Abonnenten einzeln anzugeben. Diese Verteilerlisten können auf Unternehmensverzeichnis-Servern (Microsoft Exchange, Lotus Domino usw.) geführt werden. Mit dieser Methode werden ziemlich viele Datenbankabfragen vermieden, die der Benachrichtigungsdienst ausführen muss, um Empfänger

und ihre Zustellgeräte abzurufen. Spezialisierte SMTP-Unternehmensserver sollten in der Lage sein, verfügbare Ressourcen zu nutzen und die Zustellung der Benachrichtigungsmeldungen effizienter abzuwickeln.

Minimieren der Anzahl von benutzerdefinierten Vorlagen.

IBM SPSS Collaboration and Deployment Services bietet die Möglichkeit, eine unbegrenzte Anzahl an benutzerdefinierten Vorlagen zu erstellen, die der Formatierung von Benachrichtigungsmeldungen für einen bestimmten Ereignistyp dienen. Jedoch reicht es unter normalen Umständen aus, Benachrichtigungsmeldungen nur mithilfe von Standardvorlagen zu formatieren. Die Standardvorlagen werden im Dateisystem auf dem Server gespeichert und im Arbeitsspeicher zwischengespeichert. Diese Vorlagen können an bestimmte Benutzeranforderungen angepasst werden. Für weitere Informationen siehe Thema [Bearbeiten von Benachrichtigungsvorlagen](#) auf S. 102. Eine große Anzahl an benutzerdefinierten Vorlagen (Hunderte oder Tausende pro entsprechendem Ereignis) können die Leistung spürbar beeinträchtigen, da die Vorlagen bei jeder Anforderung von der Datenbank abgerufen werden müssen und jede Benachrichtigungsmeldung separat formatiert werden muss. Dasselbe Prinzip gilt für eine benutzerdefinierte SMTP-Absenderadresse. In den meisten Fällen genügt eine einzelne Von-Standardadresse, die als Repository-Konfigurationsoption angegeben ist. Selbst wenn der Inhalt (Betreff und Text) der Benachrichtigungsvorlage identisch mit dem einer Standardvorlage ist, erzeugt eine benutzerdefinierte Von-Adresse eine benutzerdefinierte Vorlage für eine bestimmte Benachrichtigung.

Minimieren der Anzahl der Abonnements.

Zur verbesserten Leistung eines Benachrichtigungsdienstes ist es im Allgemeinen wünschenswert, die Anzahl an Abonnements zu minimieren, die einem einzigen Ereignis entsprechen. Wenn das eingehende Ereignis einer großen Anzahl an Abonnements mit unterschiedlichen Abonnenten und Meldungsvorlagen entspricht, kann das System die Verteilung nicht effizient zusammenfassen und muss separate Benachrichtigungsmeldungen für die Empfänger generieren. Es ist wichtig, zu beachten, dass ein einziges anfängliches Benachrichtigungsereignis auf dem Weg durch die Ereignistyphierarchie eine Reihe von abgeleiteten Ereignissen erzeugen kann. Ein anfängliches Ereignis kann auch durch anwendungsspezifische Ereignisaufteilungen in eine Reihe von Ereignissen zerlegt werden. Wenn für ein anfängliches Ereignis eine große Anzahl abgeleiteter Ereignisse erzeugt wird, ist eine Strategie zur Verwaltung von Abonnementlayouts empfehlenswert. Beispiel: Anstatt eine Anzahl separater Abonnements für jeden Unterordner in der Content-Repository-Hierarchie anzugeben, genügt es häufig, ein einziges Abonnement für den übergeordneten Ordner anzugeben und die Option Auf Unterordner anwenden zu aktivieren. Weitere Informationen finden Sie in der IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Benutzerdokumentation. Die Begrenzung der Anzahl von einzelnen Abonnements kann ebenfalls vorteilhaft sein. Anstatt Benutzern individuelle Abonnements zu erlauben, können auf SMTP-Unternehmensservern Verteilerlisten eingerichtet und geführt werden. Mithilfe von Verteilerlisten lässt sich eine begrenzte Anzahl an Abonnements erstellen, um die Leistung zu verbessern sowie die Meldungsverarbeitung und Verteilungszeit zu minimieren.

Planen von Aktivitäten zur Abonnementverwaltung.

Zur verbesserten Leistung beim Ereignisabgleich führt der IBM SPSS Collaboration and Deployment Services-Benachrichtigungsdienst eine Reihe von internen Caches. Diese Caches werden ungültig (gelöscht), wenn der Client Änderungen am Ereignistyp-Repository oder am Abonnement-Repository vornimmt. Es ist empfehlenswert, Aktivitäten zur Abonnementverwaltung wie Hinzufügen von Abonnenten, Löschen von Abonnements usw. auf der Grundlage eines Zeitplans auszuführen, der außerhalb der Spitzenzeiten der Ereignisverarbeitung für den Benachrichtigungsdienst liegt. Das Ausführen der Abonnementverwaltung bei geringer Verarbeitungslast ist im Allgemeinen akzeptabel, kann aber zu kurzzeitigen Leistungsabfällen führen.

Fehlersuche im Benachrichtigungsdienst

Bearbeiten Sie zur Aktivierung der Fehlersuche im Benachrichtigungsdienst die Datei *log4j.xml* auf Ihrem Anwendungsserver. Aktivieren Sie beim Einsatz von JBOSS die Protokollierungsebene **DEBUG** für das Paket *com.spss.notification*, indem Sie `<your_jboss_installation>\server\default\conf\log4j.xml` wie folgt bearbeiten:

```
<category name=com.spss.notification> <priority value=DEBUG/> </category>
```

Andere Anwendungsserver können Browser-Schnittstellen oder einige andere Bearbeitungsmöglichkeiten für die Protokollierungskonfiguration der eingesetzten Komponenten zur Verfügung stellen. Um die SMTP-Protokollierung zu aktivieren, stellen Sie die Konfigurationsoption *SMTP - Debug-Modus einschalten* in IBM® SPSS® Collaboration and Deployment Services Deployment Manager auf **true** ein. Das Benachrichtigungsprotokoll ist sehr umfangreich und bietet detaillierte Informationen zu Aktivitäten des Ereignisabgleichs und der Benachrichtigungsverteilung, aber der wichtigste Protokolleintrag, den Sie suchen sollten, ist der folgende:

```
[...SmtplibDistributor] Exiting SMTP distributor. The distribution took 5.906 s.
```

Wenn die SMTP-Verteilung länger als 100–200 Millisekunden dauert, wird dringend empfohlen, einen dedizierten SMTP-Server zu verwenden.

Zu Debugging-Zwecken ist auch empfehlenswert, "Delivery Status Notifications" (DSN) zu aktivieren, indem Sie die entsprechende Konfigurationsoption auf die folgenden Werte einstellen:

SMTP DSN Notify

FAILURE,SUCCESS,DELAY

SMTP DSN Ret

FULL

Hinweis: Ihr SMTP-Server muss die RFC3461-Spezifikation unterstützen, um diese Zustellbenachrichtigungen zu generieren.

Fehlerbehebung bei fehlgeschlagener Benachrichtigungszustellung

Wenn für den E-Mail-Server korrekte Einstellungen angegeben wurden und die E-Mail-Adresse des Standard-Absenders bei der Installation des Repository angegeben wurde, ist gewöhnlich keine zusätzliche E-Mail-Konfiguration erforderlich, damit IBM® SPSS® Collaboration and Deployment Services-Benachrichtigungen erfolgreich zugestellt werden. Wenn bei der Installation ein Fehler unterlaufen ist, kann dieser durch Ändern der Konfigurationsoptionen für Benachrichtigungen korrigiert werden. Für weitere Informationen siehe Thema [Benachrichtigung](#) in Kapitel 8 auf S. 70.

Der IBM SPSS Collaboration and Deployment Services-Administrator wird ebenfalls über die fehlgeschlagene Zustellung von Benachrichtigungen oder Abonnements mit einer systemgenerierten Meldung wie der folgenden informiert:

Your message did not reach some or all of the intended recipients.

Subject: IBM SPSS Deployment Services: New version of ChurnAnalysis created
Sent: 4/5/2010 2:35 PM

The following recipient(s) could not be reached:

jsmiht@mycompany.com on 4/5/2010 2:35 PM

There was a SMTP communication problem with the recipient's email server.
Please contact your system administrator.

In den meisten Fällen werden Zustellprobleme dadurch verursacht, dass dem Benutzer ein Fehler bei der Angabe von Benachrichtigungsempfängern oder Standard-Abonnementadressen unterläuft.

In manchen Fällen ist es möglich, dass Probleme bei der Zustellung von Benachrichtigungsmeldungen aufgrund der Einrichtung des Unternehmensnetzwerks oder des E-Mail-Servers auftreten. Beispielsweise wurde der Server eventuell nicht für die Weiterleitung an externe Adressen konfiguriert. Folgende Maßnahmen können zur Untersuchung des Problems ergriffen werden:

- Um fehlgeschlagene Benachrichtigungszustellungen definitiv zu diagnostizieren, verwenden Sie Repository-Audit-Datensätze. Weitere Informationen zu Auditing finden Sie unter Kapitel 13.
- Um die Ursache der fehlgeschlagenen Benachrichtigung zu bestimmen, sollten Sie den Debugging-Modus aktivieren. Für weitere Informationen siehe Thema [Fehlersuche im Benachrichtigungsdienst](#) auf S. 109.
- *nslookup*-Abfragen können verwendet werden, um die Konfiguration Ihres SMTP-Servers zu prüfen.
- Eine Überprüfung der SMTP-Header der Benachrichtigungsmeldungen kann nützliche Informationen zur Meldungsweiterleitung des SMTP-Servers liefern.

Fehlgeschlagene Zustellungen von Benachrichtigungen und Abonnements werden in Repository-Auditing-Ansichten protokolliert. Für weitere Informationen siehe Thema [Auditing des Repository](#) in Kapitel 13 auf S. 116.

JMS-Setup

IBM® SPSS® Collaboration and Deployment Services verwendet Java Messaging Services (JMS), um mit Drittanwendungen zu kommunizieren und Jobverarbeitungen aufgrund von IBM® SPSS® Collaboration and Deployment Services Repository-Ereignissen auszulösen. Das JMS-API ist ein Java Message Oriented Middleware- (MOM-)API für das Senden von Meldungen zwischen zwei oder mehr Clients. Mit JMS erstellt ein Programm zuerst eine Instanz einer Verbindungs-Factory, um eine Verbindung zur Warteschlange oder zum Thema aufzubauen, und füllt die Meldungen mit Daten und sendet oder veröffentlicht sie. Auf der Empfangsseite erhalten oder abonnieren die Clients dann die Meldungen. Dieselben Java-Klassen können zur Kommunikation mit unterschiedlichen JMS-Providern mithilfe der JNDI-Information für den jeweiligen Provider benutzt werden.

IBM SPSS Collaboration and Deployment Services unterstützt JMS-Kommunikation nur auf der Basis des Veröffentlichung/Abonnement-Modells, in dem Meldungen an ein bestimmtes Meldungsthema veröffentlicht werden. Null oder mehr Abonnenten können Interesse am Empfang der Meldungen zu einem bestimmten Thema registrieren. JMS-Warteschlangen werden derzeit nicht unterstützt.

Das Verfahren für die Einrichtung von JMS zur Zusammenarbeit mit IBM SPSS Collaboration and Deployment Services unterscheidet sich abhängig vom JMS-Provider, der von einer bestimmten IBM SPSS Collaboration and Deployment Services-Installation benutzt wird. Einige der beliebtesten Open-Source-JMS-Provider sind Apache ActiveMQ, OpenJMS von der OpenJMS Group und JBoss Messaging von JBoss. Zu den herstellerabhängigen Implementierungen gehören WebSphere MQ von IBM (früher MQSeries), Sun Java System Message Queue und BEA WebLogic.

Das Beispiel unten zeigt die Verwendung von JMS in IBM SPSS Collaboration and Deployment Services: Das erste Beispiel zeigt, wie ein Beispielprogramm für die Kommunikation mit IBM SPSS Collaboration and Deployment Services unter Verwendung von JBoss Messaging konfiguriert wird; das Beispiel enthält eine JMS-Thema-Konfigurationsdatei, den Quellcode einer Java-Klasse, die JMS-Meldungen an das Thema veröffentlicht wird sowie eine Windows-Stapeldatei zur Ausführung der Klasse. Das zweite Beispiel zeigt die Einrichtung der Jobverarbeitung aufgrund von Repository-Ereignissen. Informationen über das Einrichten anderer JMS-Provider finden Sie in der Dokumentation des jeweiligen Anbieters.

JMS-Thema-Konfiguration

In JBoss werden JMS-Warteschlangen und -Themen als **verwaltete Objekte** bezeichnet, die durch Konfigurationsdateien bereitgestellt werden können. Beispiel:

```
<?xml version=1.0 encoding=UTF-8?>
```

```

<server>
  <mbean code=org.jboss.mq.server.jmx.Topic
    name=jboss.mq.destination:service=Topic,name=PEStestTopic>
    <depends optional-attribute-name=DestinationManager>jboss.mq:service=DestinationManager</depends>
  </mbean>

</server>

```

Diese Datei muss im Verzeichnis `%JBOSS_HOME%/server/default/deploy` abgelegt werden und das Repository muss neu gestartet werden. Das Thema wird an den jndi-Namen `topic/PEStestTopic` gebunden.

JBoss wird mit vorkonfigurierten Warteschlangen und Themen geliefert. Diese Einstellungen befinden sich in der Datei `jbossmq-destinations-service.xml`, die im Verzeichnis `%JBOSS_HOME%/server/default/deploy/jms` abgelegt ist.

IBM SPSS Collaboration and Deployment Services-Setup

So konfigurieren Sie IBM® SPSS® Collaboration and Deployment Services für die Kommunikation mit dem JMS-Service:

1. Richten Sie mithilfe von IBM® SPSS® Collaboration and Deployment Services Deployment Manager eine Meldungsdomäne ein, die auf `PEStestTopic` verweist.
2. Erstellen Sie einen meldungsbasierten Zeitplan für einen IBM SPSS Collaboration and Deployment Services-Job, der die Domäne verwendet. Weitere Informationen finden Sie im Deployment Manager-Benutzerhandbuch.

JMS-Client-Beispielprogramm

`SendMessageClientMain.java` ist ein Beispielprogramm, das Meldungen an das Thema `topic/PEStestTopic` veröffentlicht, um anschließend IBM® SPSS® Collaboration and Deployment Services-Verarbeitung auszulösen.

```

import java.util.Properties;

import javax.jms.Connection;
import javax.jms.MessageProducer;
import javax.jms.Session;
import javax.jms.Topic;
import javax.jms.TopicConnectionFactory;
import javax.jms.TopicSession;
import javax.jms.TextMessage;
import javax.naming.InitialContext;
import javax.naming.Context;

public class SendMessageClientMain
{
    public static void main(String args[])
        throws Exception
    {

```



```
System.out.println(SendMessageClient...);
Connection connection = null;
Session session = null;
Topic topic = null;

// Diese beiden Zeilen so ändern, dass sie zum korrekten Thema und der zu sendenden Meldung weisen
String topicName = topic/PEStestTopic;
String messageText = testmsg;

Properties props = new Properties();
// Diese beiden Zeilen so ändern, dass sie zum korrekten JMS-Server weisen.
props.put(Context.INITIAL_CONTEXT_FACTORY, org.jnp.interfaces.NamingContextFactory);
props.put(Context.PROVIDER_URL, jnp://localhost:1099);

try {
    InitialContext iniCtx = new InitialContext(props);
    Object tmp = iniCtx.lookup(ConnectionFactory);
    TopicConnectionFactory tcf = (TopicConnectionFactory) tmp;

    connection = tcf.createConnection();
    topic = (Topic) iniCtx.lookup(topicName);
    session = connection.createSession(false,
        TopicSession.AUTO_ACKNOWLEDGE);
    connection.start();

    // Textmeldung senden
    MessageProducer send = session.createProducer(topic);
    TextMessage tm = session.createTextMessage(messageText);
    send.send(tm);
    System.out.println(sendMessage - sent text= + tm.getText());
    send.close();
    System.out.println(End TopicSendClient);

    connection.stop();
    session.close();
    connection.close();
}
catch (Exception e)
{
    // Fehlerbehandlung als Übung für Kursteilnehmer.
    e.printStackTrace();
}

System.exit(0);
}
```

Das Meldungsthema, der Meldungstext und die Fehlerbehandlungsroutinen können wie erforderlich geändert werden. Anstatt die Eigenschaften `Context.INITIAL_CONTEXT_FACTORY` und `Context.PROVIDER_URL` im Quellcode festzulegen, kann die Datei *jndi.properties* wie folgt erstellt werden, um zu definieren, wie das Nachschlagen auf dem JMS-Server erfolgt:

```
java.naming.provider.url=jnp://localhost:1099
java.naming.factory.initial=org.jnp.interfaces.NamingContextFactory
```

Die Datei muss in den Pfad der kompilierten Klasse des Beispielprogramms platziert werden.

Ausführen des Beispielprogramms

Folgendes ist ein Beispiel für eine Windows-Stapeldatei zur Veröffentlichung einer JMS-Meldung an JBoss-Messaging-Service durch Ausführen von *SendMessageClientMain.class*. Beachten Sie, dass die Stapeldatei Umgebungsvariablen so einstellt, dass sie auf die geeignete JMS-Naming-Factory-Klasse zeigen, bevor das Beispielprogramm gestartet wird.

```
set JBOSS_HOME=C:\ssk\pgms\pes35\jboss\4.0.3SP1

set JBOSS_SERVER_LIB=%JBOSS_HOME%\server\default\lib
set JBOSS_ROOT_LIB=%JBOSS_HOME%\lib

set CLASSPATH=.;\bin
set CLASSPATH=%CLASSPATH%;%JBOSS_SERVER_LIB%\jboss-j2ee.jar
set CLASSPATH=%CLASSPATH%;%JBOSS_SERVER_LIB%\log4j.jar
set CLASSPATH=%CLASSPATH%;%JBOSS_SERVER_LIB%\jnpserver.jar
set CLASSPATH=%CLASSPATH%;%JBOSS_ROOT_LIB%\jboss-common.jar
set CLASSPATH=%CLASSPATH%;%JBOSS_SERVER_LIB%\jbossmq.jar
set CLASSPATH=%CLASSPATH%;%JBOSS_SERVER_LIB%\jboss.jar
set CLASSPATH=%CLASSPATH%;%JBOSS_ROOT_LIB%\jboss-system.jar
set CLASSPATH=%CLASSPATH%;%JBOSS_ROOT_LIB%\concurrent.jar

java SendMessageClientMain
```

Wenn alle vorangehenden Schritte korrekt abgeschlossen wurden, löst die Ausführung von *SendMessageClientMain.class* die Verarbeitung des entsprechenden meldungsbasierten IBM® SPSS® Collaboration and Deployment Services-Jobzeitplans aus.

Beispiel für meldungsbasierte Verarbeitung

Die meldungsbasierte Planungsfunktion von IBM® SPSS® Collaboration and Deployment Services kann verwendet werden, um die Verarbeitung durch Repository-Ereignisse und durch Drittanwendungen auszulösen. Zum Beispiel kann ein Job so konfiguriert werden, dass er erneut ausgeführt wird, sobald der in einem der Jobschritte verwendete IBM® SPSS® Modeler-Stream aktualisiert wird. Dieses Verfahren beinhaltet die folgenden Schritte:

- ▶ Erstellen Sie über IBM® SPSS® Collaboration and Deployment Services Deployment Manager eine JMS-Meldungsdomäne.

-
- ▶ Richten Sie mithilfe der Meldungsdomäne einen meldungsbasierten Zeitplan für den Job ein. Beachten Sie, dass die Meldungsauswahl die Ressourcen-ID des SPSS Modeler-Streams wie im folgenden Beispiel angeben muss:

ResourceID=<resource ID>

Die Repository-Ressourcen-ID des SPSS Modeler-Streams befindet sich in den Objekteigenschaften.

- ▶ Richten Sie auf Basis des von Ihnen definierten JMS-Abonnenten eine Benachrichtigung für den SPSS Modeler-Stream ein.
- ▶ Um den meldungsbasierten Zeitplan zu testen, muss der Stream in SPSS Modeler geöffnet, geändert und im Repository gespeichert werden. Wenn alles korrekt eingestellt wurde, wird der Zeitplan den Job auslösen.

Auditing des Repository

Während sich der Inhalt der gesammelten und erstellten Datenobjekte vermehrt, ist es erforderlich, das Verhalten der Daten zu verfolgen. Mithilfe von Datenbank-Auditing können Sie das Wer, Was, Wann und Wie der Datenobjekte nachvollziehen - wer mit den Daten interagiert hat, auf welche Datenobjekte zugegriffen wurde, wann die Aktion stattfand und wie diese Objekte manipuliert wurden.

Abhängig von der benötigten Detailebene bietet das IBM® SPSS® Collaboration and Deployment Services Repository einen komfortablen Mechanismus zur Beantwortung dieser Fragen, der so flexibel ist, dass so viele oder so wenige Details wie gewünscht gesammelt werden können. Datenbankberichte und -Audits können anfangs einfach gehalten werden und mit geänderten Geschäftsanforderungen komplexer werden.

Anmerkung: Auf täglicher Basis können Änderungen an Repository-Objekten und Verarbeitungsergebnisse durch Benachrichtigungen und Abonnements verfolgt werden. Weitere Informationen finden Sie in der IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Dokumentation.

Mithilfe der Praxis von Datenbank-Auditing und -Berichterstellung können Sie:

- Änderungen überwachen, z. B. die Erstellung und das Entfernen von Datenobjekten, die in der Datenbank gespeichert sind.
- Diese Datenbankaktivität für zukünftige Analysen und Referenzen aufzeichnen oder protokollieren.
- Berichte über Datenbankaktivitäten generieren.

Die Fähigkeit, diese Aktionen einfach zu verfolgen, verleiht dem Benutzer eine bessere Kontrolle über die Daten und gewährleistet die Einhaltung der Unternehmensrichtlinien für Datensicherheit und Änderungsverfolgung.

Datenbank-Audit-Möglichkeiten

Das Repository bietet mehrere Datenbanktabellen zur Aufzeichnung von Systemereignissen und Objektänderungen. Wenn das Repository in einer unterstützten relationalen Datenbank installiert wird, werden die erforderlichen Tabellen für Auditing und Berichterstellung automatisch angelegt. Der Benutzer muss keine Datenbankobjekte manuell füllen.

Die einfachste Möglichkeit, auf Auditing-Informationen zuzugreifen, ist die Ausführung von SQL-Abfragen in einer unterstützten Datenbank-Clientanwendung. Beispielsweise können mit BIRT Report Designer for IBM® SPSS®, das in der IBM® SPSS® Collaboration and Deployment Services-Installation enthalten ist, Auditing-Berichte erstellt werden.

Wenn bestimmte Arten von Auditing-Informationen regelmäßig abgerufen werden müssen, können Ansichten eingerichtet werden. Eine Datenbankansicht ist eine schreibgeschützte oder virtuelle Tabelle, die aus dem Ergebnis einer Abfrage besteht. Im Unterschied zu normalen Tabellen in einer relationalen Datenbank ist eine Ansicht nicht Teil des physischen Schemas, sondern eine dynamische Tabelle, die aus Daten in der Datenbank berechnet oder zusammengestellt wird. Das Ändern der Daten in der Tabelle ändert die in der Ansicht gezeigten Daten.

Das Repository wird mit mehreren vordefinierten Ansichten installiert, mit deren Hilfe sich eine Vielzahl von Auditing-Informationen über Repository-Objekte abrufen lässt, z. B. Dateien, Jobs, Streams usw. Benutzerdefinierte Ansichten können für komplexere Anforderungen an die Berichterstellung eingerichtet werden. Beachten Sie beim Implementieren von benutzerdefinierten Ansichten Varianten der SQL-Syntax in der Originaldokumentation des Datenbankherstellers.

Hinweis: Audit-Abfragen können an IBM SPSS Collaboration and Deployment Services-Ereignistabellen und vordefinierten Ansichten ausgeführt werden. Da sich die Tabellenstruktur jedoch in späteren Systemversionen ändern kann, empfiehlt es sich aus Kompatibilitätsgründen beim Schreiben von Audit-Abfragen Ansichten anstelle von Tabellen zu verwenden.

Audit-Ereignisse

Die folgenden Systemereignisse lösen Einträge in die Datenbankereignistabellen aus:

Repository-Ereignisse

- Erstellen einer Datei oder eines Ordners
- Aktualisieren einer Datei oder eines Ordners
- Version
- Löschen einer Datei oder eines Ordners
- Ändern der Berechtigungen für eine Datei oder einen Ordner

Sicherheitsereignisse

- Erfolgreiche Anmeldung
- Fehlgeschlagene Anmeldung
- Hinzufügen eines Benutzers
- Löschen eines Benutzers
- Ändern eines Kennworts
- Hinzufügen einer Gruppe
- Hinzufügen eines Benutzers zu einer Gruppe
- Löschen einer Gruppe

Job-Ausführungseignisse

- Übergeben eines Jobs
- Starten eines Jobs

- Starten eines Jobschritts
- Erfolgreicher Abschluss eines Jobs
- Fehlgeschlagener Job
- Erfolgreicher Jobschritt
- Fehlgeschlagener Jobschritt

Scoring-Ereignisse

- Scoring-Anforderung
- Scoring-Konfigurationsänderung

Ereignistabellen

Informationen zu Repository-Ereignissen werden in Audit-Ereignis-Tabellen (SPSSAUDIT_EVENTS) und Ereignisparameter-Tabellen (SPSSAUDIT_PARAMETERS) gespeichert. Jedes Systemereignis generiert eine Zeile in der Tabelle SPSSAUDIT_EVENTS. Ein Ereignis kann verknüpfte Parameterzeilen in der Tabelle SPSSAUDIT_PARAMETERS enthalten (nur 1:n-Beziehung).

Audit-Ereignis-Tabelle (SPSSAUDIT_EVENTS)

SERIAL. Die eindeutige ID für die Ereigniszeile. Die Nummer kann verwendet werden, um die Reihenfolge zu bestimmen, in der die Ereignisse generiert wurden.

STAMP. Datum und Uhrzeit, an denen das Ereignis eingetreten ist.

COMPONENT. Die Systemkomponente, von der das Ereignis stammt. Folgende Werte können für COMPONENT zurückgegeben werden:

- repository/audit_component_name—Repository-Ereignis
- security/componentAuthN—Benutzerauthentifizierungs-Ereignis
- security/componentLRU—Benutzer- und Gruppen-Setup-Ereignis
- prms/prms—Jobplanungs-Ereignis
- notification/notification—Benachrichtigungs- oder Abonnement-Ereignis
- userpref/auditComponent—Ereignis für Änderung von Benutzervoreinstellungen
- scoring/scoring—Scoring-Serviceereignis

LOCUS. Definiert durch die Komponente "owner"; weist einen spezifischeren Ereignistyp zu. Folgende Werte können für LOCUS zurückgegeben werden:

Locus-Codes für Repository-Ereignisse

- repository/audit_access_object—Datei oder Ordner, auf die/den zugegriffen wurde
- repository/audit_new_object—Datei oder Ordner erstellt
- repository/audit_update_object—Datei oder Ordner aktualisiert (Inhalt oder Metadaten)
- repository/audit_new_version—Eine Version erstellt

- repository/audit_delete_version—Eine Version gelöscht
- repository/audit_delete_object—Datei oder Ordner gelöscht
- repository/audit_move_object—Datei oder Ordner verschoben
- repository/audit_modify_permissions—Berechtigungen auf eine geänderte Datei oder einen geänderten Ordner
- repository/audit_update_custom_property_value—Benutzerdefinierter Eigenschaftswert einer Datei oder eines Ordners aktualisiert
- repository/audit_new_custom_property—Neue benutzerdefinierte Eigenschaft erstellt
- repository/audit_modify_custom_property—Bestehende benutzerdefinierte Eigenschaft geändert
- repository/audit_delete_custom_property—Bestehende benutzerdefinierte Eigenschaft gelöscht
- repository/audit_reindex_repository_started—Repository-Neuindizierungsprozess gestartet
- repository/audit_reindex_repository_ended—Repository-Neuindizierungsprozess beendet

Locus-Codes für Sicherheitsereignisse

- security/locAuthen—Erfolgreiche Anmeldung
- security/locNotAuthen—Fehlgeschlagene Anmeldung
- security/locLogout—Abmeldung
- security/locLRUAdd—Benutzer hinzugefügt
- security/locLRUDelete—Benutzer gelöscht
- security/locLRUUpdate—Passwortänderung
- security/locLRUAdd—Gruppe hinzugefügt
- security/locLRUUpdate—Gruppe umbenannt
- security/locLRUUpdate—Benutzer zu Gruppe hinzugefügt/aus Gruppe gelöscht
- security/locLRUDelete—Gruppe gelöscht

Locus-Codes für Job-Ausführungsereignisse

- prms/audit_job_submit—Job übergeben
- prms/audit_job_start—Job gestartet
- prms/audit_job_step_start—Starten eines Jobschritts
- prms/audit_job_success—Job wird erfolgreich beendet
- prms/audit_job_failure—Job schlägt fehl
- prms/audit_job_step_success—Jobschritt wird erfolgreich beendet
- prms/audit_job_step_failure—Jobschritt schlägt fehl
- prms/audit_job_update—Job aktualisiert

Locus-Codes für Benachrichtigungsereignisse

- notification/audit_delivery—Zustellereignis für Benachrichtigungsmeldung (zugestellt, nicht zugestellt oder teilweise zugestellt)
- notification/audit_subscription—Änderungereignis für Benachrichtigungs- oder Abbonnementeinstellungen (Abonnement erstellt, aktualisiert oder gelöscht)

Locus-Codes für Benutzervoreinstellungs-Ereignisse

- userpref/auditLSet—Benutzervoreinstellungswert festgelegt
- userpref/auditLDelete—Benutzervoreinstellungswert gelöscht

Locus-Codes für Scoring-Serviceereignisse

- scoring/metric_update—Scoring-Serviceanforderung oder Scoring-Konfigurationsaktualisierung

MIMETYPE. MIME-Typ des Objekts, das mit dem Ereignis verknüpft ist.

TITLE. Kurzbeschreibung des Ereignisses, gewöhnlich in Ereignislisten angezeigt. Für Content-Repository-Ereignisse ist dies der Name der Datei.

PRINCIPALID. Der Benutzer, der das Ereignis generiert hat.

AUDIT_RESOURCE. Falls mit Inhalt verbunden, ist dies der URI des Content-Repository-Objekts.

DETAILS. Ein String, der zusätzliche komponentendefinierte Informationen zu dem Ereignis liefert, z. B. ein altes Label bei einer Label-Änderung, alte Metadaten bei einer Metadatenänderung und den alten Namen bei einer Namensänderung.

SIGNATURE. Signatur, die zur Gültigkeitsbestätigung von Daten verwendet wird.

ADDRESS. IP-Adresse des Clientsystems, das mit dem Ereignis verknüpft ist.

Audit-Ereignisparameter-Tabelle (SPSSAUDIT_PARAMETERS)

SERIAL. Der Fremdschlüssel zur Tabelle SPSSAUDIT_EVENTS, die den Parameter mit dem Ereignis verknüpft.

NAME. Beschreibender Name für den Parameter—z. B. JobExecutionID, JobID, JobStepID, JobName, JobStepName usw.

VALUE. Wert des genannten Parameters.

Nutzen Sie Tools der Datenbank-Clientanwendung, um zusätzliche Informationen zu den Eigenschaften von Ereignistabellen zu beziehen, z. B. Spaltendatentypen und "Nullability".

Audit-Ansichten

Die folgenden Audit-Ansichten werden bei der Installation des Repository standardmäßig in der Datenbank erstellt. Nutzen Sie Tools der Datenbank-Clientanwendung, um zusätzliche Informationen zu den Eigenschaften der Ansichten zu beziehen. Das Auditing von

Datenbankobjekten erfolgt über die Ausführung von SQL-Abfragen in den Ansichten. Beachten Sie, dass die Repository-Datenbank auch eine Reihe anderer Ansichten enthält, die zur Unterstützung von Audit-Ansichten verwendet werden. Die Unterstützungsansichten sind nicht für Berichterstellungen vorgesehen.

Audit (SPSSPLAT_V_AUDIT)

Die Audit-Ansicht enthält Auditing-Informationen aus der Ansicht "Dateiversion". Diese Ansicht enthält eine Zeile für jeden Audit-Parameter für jedes Audit-Ereignis.

AUDITSERIALNUMBER. Die eindeutige ID für das Ereignis. Die Nummer kann verwendet werden, um die Reihenfolge zu bestimmen, in der die Ereignisse generiert wurden.

AUDITTIMESTAMP. Der Audit-Zeitstempel (bzw. das Datum der Ereigniserstellung) wird durch die generierende Komponente festgelegt.

AUDITCOMPONENT. Der Name der Komponente oder des Subsystems, durch das das Ereignis erstellt wurde und für das Auditing durchgeführt wird. Das Format ist in der Form `com.spss.<Komponente>`.

AUDITCATEGORY. Die Kategorie der Ereignisse, für die Auditing durchgeführt wird.

MIMETYPE. Der MIME-Typ des Objekts, für das Auditing durchgeführt wird.

AUDITTITLE. Name der Kategorie oder des Objekts, für das Auditing durchgeführt wird.

AUDITPRINCIPAL. Der Principal-Benutzer des Objekts, für das Auditing durchgeführt wird.

AUDITRESOURCE. Der Content-Host, für den Auditing durchgeführt wird, z. B. die Content-Repository-Ressourcen-ID.

AUDITDETAILS. Ein String, der zusätzliche komponentendefinierte Informationen zu dem Ereignis liefert, z. B. ein altes Label bei einer Label-Änderung, alte Metadaten bei einer Metadatenänderung und den alten Namen bei einer Namensänderung.

ADDRESS. IP-Adresse des Clientsystems, das mit dem Ereignis verknüpft ist.

AUDITPARAMETERNAME. Ein erweiterter Parameter des Audit-Ereignisses—z. B. `JobStepExecutionID`, `JobExecutionID` oder `JobID`.

AUDITPARAMETERVALUE. Ein erweiterter Parameterwert des Audit-Ereignisses—z. B. der ID-Wert.

AUDITRESOURCEID Die Repository-ID der Ressource, die mit dem Ereignis verknüpft ist. Fremdschlüssel zur Datei- oder Job-ID in der Ansicht "Dateiversion" (`SPSSPLAT_V_FILEVERSION`).

AUDITMARKER Ressourcenversion, die mit dem Ereignis verknüpft ist. Fremdschlüssel zum Datei- oder Jobversionskennzeichen in der Ansicht "Dateiversion" (`SPSSPLAT_V_FILEVERSION`).

Benutzerdefinierte Eigenschaft (SPSSPLAT_V_CUSTOMPROPERTY)

Die Ansicht "Benutzerdef. Eigenschaft" präsentiert die Informationen der benutzerdefinierten Eigenschaft für die Zeilen in der Ansicht "Dateiversion" (1:n-Beziehung).

PROPERTYNAME. Der Name der benutzerdefinierten Eigenschaft.

PROPERTYVALUE. Der Wert der benutzerdefinierten Eigenschaft.

FILEID. Fremdschlüssel zur Datei oder zum Job in der Ansicht "Dateiversion", für die diese Eigenschaft gilt.

Dateiversion (SPSSPLAT_V_FILEVERSION)

Die Ansicht "Dateiversion" präsentiert Datei- und Versionsinformationen für Repository-Objekte wie IBM® SPSS® Modeler-Streams, IBM® SPSS® Statistics-Syntaxdateien, SAS-Syntaxdateien usw. Diese Ansicht enthält eine Zeile für jede Version von jeder Datei, jedem Ordner oder jedem Job.

FILEID. Die eindeutige ID der Datei.

VERSION. Die Version der Datei.

FILENAME. Der Name der Datei.

VERSIONMARKER. Das Versionskennzeichen der Dateiversion.

VERSIONLABEL. Das Versions-Label der Dateiversion.

FILEPATH. Der Pfad zur Datei.

MIMETYPE. Der MIME-Typ der Datei.

AUTHOR. Der (vom Benutzer angegebene) Autor der Datei.

DESCRIPTION. Die Beschreibung der Datei.

FILECREATEDDATE. Datum und Uhrzeit, an denen die Datei erstellt wurde.

FILECREATEDBY. Der Benutzer, der die Datei erstellt hat.

FILELASTMODIFIEDDATE. Datum und Uhrzeit, an denen die Datei zuletzt geändert wurde.

FILELASTMODIFIEDBY. Der Benutzer, der die Datei zuletzt geändert hat.

VERSIONCREATEDDATE. Datum und Uhrzeit, an denen die Dateiversion erstellt wurde.

VERSIONCREATEDBY. Der Benutzer, der die Version der Datei erstellt hat.

VERSIONLASTMODIFIEDDATE. Datum und Uhrzeit, an denen die Dateiversion zuletzt geändert wurde.

VERSIONLASTMODIFIEDBY. Der Benutzer, der die Version zuletzt geändert hat.

Jobverlauf (SPSSPLAT_V_JOBHISTORY)

Die Ansicht "Jobverlauf" präsentiert Informationen zur Ausführung von Jobschritten. Diese Ansicht enthält eine Zeile für jede Ausführung eines jeden Jobschritts in jedem Job.

EXECUTIONID. Die eindeutige ID der Ausführung.

JOBID. Fremdschlüssel zum Job (FILEID) in der Ansicht "Dateiversion".

JOBVERSION. Fremdschlüssel zur Jobversion in der Ansicht "Dateiversion".

JOBSTEPID. Fremdschlüssel zum Jobschritt in der Ansicht "Jobschritt".

JOBSTEPEXECUTIONSTATUS. Der Status des Jobschritts hinsichtlich Erfolg/Fehlschlag.

JOBSTEPEXECUTIONSTARTED. Die Startzeit des Jobschritts.

JOBSTEPEXECUTIONENDED. Die Endzeit des Jobschritts.

JOBSTEPEXECUTIONRUNTIME. Die Gesamtlaufzeit des Jobschritts.

JOBSTEPERRORLOG. Die ID der Fehlerprotokolldatei für den Jobschritt.

JOBEXECUTIONSTATUS. Der Status des Jobs hinsichtlich Erfolg/Fehlschlag. Folgende Werte können für JOBEXECUTIONSTATUS zurückgegeben werden:

- Null—Unbekannt
- 0—Fehlgeschlagen
- 1—Erfolg
- 2—In Warteschlange
- 3—In Verarbeitung
- 4—Beendet
- 5—Weiterleitung
- 6—Fehler
- 7—Weiterleitungsfehler
- 8—Mit Abbruchsanforderung
- 9—Abgebrochen
- 10—Abbruch steht bevor
- 11—Weiterleitung abgebrochen
- 12—Per Join verbinden

JOBEXECUTIONSTARTED. Die Startzeit des Jobs.

JOBEXECUTIONENDED. Die Endzeit des Jobs.

JOBEXECUTIONRUNTIME. Die Gesamtlaufzeit des Jobs.

JOBCLUSTERQUEUEDDATETIME. Der Zeitpunkt, an dem der Job in die Warteschlange gesetzt wurde. Der Zeitpunkt für die Einreihung in die Warteschlange liegt etwas später als der Zeitpunkt für die Übergabe des Jobs.

JOBCLUSTERCOMPLETIONCODE. Abhängig vom Jobtyp ist dies ein ganzzahliger Wert, der dem Jobstatus entspricht. Null (0) gibt den Erfolg für alle Jobtypen an.

JOBCLUSTERAPPLICATIONSTATUS. Abhängig vom Jobtyp ist dies ein Stringwert, der dem Jobstatus entspricht.

JOBPROCESSID. Abhängig vom Jobtyp ist dies die ID des entsprechenden Systemprozesses—z. B. die ID eines Betriebssystemprozesses für die Ausführung einer ausführbaren Datei.

JOBEXECUTEDPARAMETERS. Dieses Feld wird derzeit nicht verwendet.

JOBNOTIFICATIONENABLED. Gibt an, ob Benachrichtigungen für den Job aktiviert sind.

Jobschritt (SPSSPLAT_V_JOBSTEP)

Die Ansicht “Jobschritte” enthält Informationen über Jobschritte in Jobs. Diese Ansicht enthält eine Zeile für jeden Jobschritt einer jeden Version jedes Jobs.

JOBSTEPID. Die eindeutige ID des Jobschritts.

JOBSTEPNAME. Der Name des Jobschritts.

JOBID. Fremdschlüssel zum Job (FILEID) in der Ansicht “Dateiversion”, die diesen Jobschritt enthält.

JOBVERSION. Fremdschlüssel zur Jobversion in der Ansicht “Dateiversion”, die diesen Jobschritt enthält.

JOBSTEPTYPE. Der Typ des Jobschritts. Derzeit gibt es die Typen ClementineStreamWork, SPSSSyntaxWork, SASSyntaxWork, ExecutableContentWork (Allgemeine Arbeit) und WindowsCommandWork. Zugehörige DOS-Befehle können den Typ WindowsCommandWork oder ExecutableContentWork haben.

REFERENCEDFILEID. Die ID der von diesem Jobschritt referenzierten Datei, falls zutreffend—z. B. ein IBM® SPSS® Modeler-Stream, eine IBM® SPSS® Statistics- oder SAS-Syntaxdatei usw.

REFERENCEDFILELABEL. Das Label der Datei, die von diesem Jobschritt referenziert wird, falls zutreffend.

Zeitplan (SPSSPLAT_V_SCHEDULE)

Die Ansicht “Zeitplan” präsentiert die Zeitplaninformationen, die mit einem Job in der Ansicht “Dateiversion” verknüpft sind. Diese Ansicht enthält eine Zeile für jeden Zeitplan.

JOBID. Fremdschlüssel zum Job (FILEID) in der Ansicht “Dateiversion”.

JOBVERSION. Fremdschlüssel zur Jobversion in der Ansicht “Dateiversion”. Dies ist die Version des Jobs, der zu diesem Zeitpunkt ausgeführt werden soll. Wenn das Job-Label verschoben wird (oder eine neue Jobversion gespeichert und der Zeitplan auf die Ausführung des neuesten Jobs eingestellt wird), ändert sich die Jobversion.

SCHEDULEDFREQUENCY. Die Wiederholung des Zeitplans erfolgt gemäß dem geplanten Intervall und den entsprechenden Zeiteinheiten. Wenn beispielsweise die Häufigkeit “Täglich” und das Intervall 1 ist, dann kann der geplante Wochentag ein beliebiger Tag von Sonntag bis Samstag sein, wohingegen der geplante Tag des Monats 0 ist.

SCHEDULEDINTERVAL. Die Anzahl der Intervalle, die zwischen Zeitplänen übersprungen werden sollen. Die Bedeutung ändert sich auf der Basis des Wertes von SCHEDULEDFREQUENCY—z. B. bedeutet die Häufigkeit “Wöchentlich” mit einem Intervall von 4, dass die Ausführung jede vierte Woche erfolgt.

SCHEDULEDDAYOFMONTH. Der Tag des Monats für monatliche Zeitpläne.

SCHEDULEDDAYOFWEEK. Der Tag der Woche für wöchentliche Zeitpläne.

SCHEDULEDTIME. Die geplante Uhrzeit für den Start des Jobs.

SCHEDULESTARTDATE. Das Startdatum für regelmäßig wiederholte Zeitpläne (täglich, wöchentlich, monatlich) oder das Ausführungsdatum für andere Zeitpläne.

SCHEDULEENDDATE. Das Enddatum der Wiederholung für regelmäßig wiederholte Zeitpläne des Typs “Täglich”, “Wöchentlich”, “Monatlich”. Diese Spalte ist für die anderen Zeitpläne null und kann für die aufgelisteten Zeitpläne null sein, wenn der Zeitplan am aufgelisteten Datum nicht mehr ausgelöst werden soll.

NEXTSCHEDULEDTIME. Das nächste Startdatum des Zeitplans. Es ist null, wenn der Zeitplan sein Enddatum überschritten hat oder ein Einmal-Zeitplan ist.

SCHEDULEENABLED. Zeitplan aktiviert.

SCHEDULELABEL. Label des Jobs, der beim Auslösen des Zeitplans ausgeführt werden soll.

SCHEDULELASTUPDATE. Der Zeitstempel für das Datum, an dem dieser Zeitplan zuletzt geändert wurde.

SCHEDULECREATOR. Die Benutzer-ID der Person, die den Zeitplan erstellt hat.

Stream-Attributwert (SPSSPLAT_V_STREAMATTRVALUE)

Die Ansicht “Stream-Attributwert” präsentiert die Attributinformationen zu den Knoten in einem IBM® SPSS® Modeler-Stream. Diese Ansicht enthält eine Zeile für jeden zulässigen Wert eines jeden Attributs in jedem Stream.

ATTRIBUTEID. Die eindeutige ID des Attributs.

ATTRIBUTENAME. Der Name des Attributs.

NODEID. Fremdschlüssel zum Knoten in der Ansicht “Stream-Knoten”.

ATTRIBUTETYPE. Der Attributtyp.

ATTRIBUTE CATEGORICALVALUE. Ein zulässiger Wert für das Attribut für Attribute mit mehreren Werten.

NUMERICALUPPERBOUND. Der zulässige obere Grenzwert für numerische Attribute.

NUMERICALLOWERBOUND. Der zulässige untere Grenzwert für numerische Attribute.

Stream-Knoten (SPSSPLAT_V_STREAMNODE)

Die Ansicht “Stream-Knoten” präsentiert die Informationen für die Knoten in IBM® SPSS® Modeler-Streams. Diese Ansicht enthält eine Zeile für jeden Knoten in jeder Version eines jeden Streams.

NODEID. Die eindeutige ID des Knotens im Stream.

STREAMID. Fremdschlüssel zum Stream (FILEID) in der Ansicht “Dateiversion”, die diesen Knoten enthält.

STREAMVERSION. Fremdschlüssel zur Stream-Version in der Ansicht “Dateiversion”, die diesen Knoten enthält.

NODENAME. Der Name des Knotens im Stream.

NODETYPE. Der Typ des Knotens im Stream.

NODELABEL. Das Label des Knotens im Stream.

ALGORITHMNAME. Der Algorithmus des Knotens für Modellierungsknoten.

MININGFUNCTION. Die Data-Mining-Funktion des Knotens für Modellierungsknoten.

IOFILENAME. Die Eingabe- oder Ausgabedatei des Knotens für FileInput- oder FileOutput-Knoten.

IODATABASETABLE. Der Name der Datenbanktabelle für DatabaseInput- oder DatabaseOutput-Knoten.

IODSN. Der Name der Datenquelle des Knotens für DatabaseInput- oder DatabaseOutput-Knoten.

Hinweis: In dieser Version wird die Spalte ioDSN in der Ansicht SPSSPLAT_V_STREAMNODE nicht verwendet. Diese Spalte enthält NULL für jeden Datensatz.

Scoring-Serviceprotokollierung

IBM® SPSS® Collaboration and Deployment Services bietet außerdem Datenbankmöglichkeiten zur Protokollierung des Betriebs der Services für IBM® SPSS® Collaboration and Deployment Services - Scoring. Die folgenden Datenbankobjekte werden zur Speicherung der Scoring-Service-Daten verwendet:

- Protokollierungstabelle für Anforderungen
- Datenbankansichten
- XML-Schema

Scoring-Serviceprotokollierung wird auf allen Datenbankmanagementsystemen unterstützt, die für das Repository verwendet werden können:

- DB2
- MS SQL Server
- Oracle

Anmerkung: DB2 auf IBM i kann nicht für die Scoring-Serviceprotokollierung verwendet werden.

Protokollierungstabelle für Anforderungen

Standardmäßig werden die Scoring-Serviceanforderungsdaten in der Tabelle SPSSSCORE_LOG gespeichert.

Scoring-Protokollierungstabelle (SPSSSCORE_LOG)

SERIAL. Die eindeutige ID der Scoring-Serviceanforderung.

STAMP. Datum und Uhrzeit der Scoring-Serviceanforderung.

INFO. Zusätzliche Informationen zur Scoring-Anforderung im XML-Format. Die Informationen werden gemäß dem bei der Datenbank registrierten XML-Schema erzeugt. Dieselben Informationen sind im relationalen Format über die Scoring-Protokollansicht verfügbar.

Bereinigung und Wartung

Im Lauf der Protokollierung von Scoring-Serviceanforderungen kann die Tabelle SPSSSCORE_LOG sehr umfangreich werden, so dass unter Umständen Datensätze aus dieser Tabelle gelöscht werden müssen. Beispielsweise kann der Administrator alte Datensätze aus der Zeit vor dem 1. Januar 2009 durch Ausführung der folgenden SQL-Anweisung entfernen:

```
DELETE FROM spssscore_log WHERE STAMP < '2009-01-01'
```

Datenbankansichten

Die folgenden Scoring-Ansichten werden bei der Installation des Repository standardmäßig in der Datenbank erstellt. Sie zeigen die im XML-Format in der Spalte INFO der Tabelle SPSSSCORE_LOG gespeicherten Informationen im relationalen Format an. Nutzen Sie Tools der Datenbank-Clientanwendung, um zusätzliche Informationen zu den Eigenschaften der Ansichten zu beziehen, oder führen Sie SQL-Abfragen durch.

Scoring-Anforderung (SPSSSCORE_V_LOG_HEADER)

Diese Ansicht enthält eine Zeile für jede Scoring-Anforderung in der Tabelle SPSSSCORE_LOG table.

SERIAL. Die eindeutige ID der Scoring-Anforderung.

ADDRESS. Die IP-Adresse für den Rechner, der die Scoring-Anforderung initiiert. Beachten Sie, dass dies in bestimmten Fällen die Adresse des Servers anstelle des Clients sein kann, z. B. die Adresse des Cluster-Lastenausgleichs oder Proxy-Servers.

HOSTNAME. Der Name des Rechners, der die Scoring-Anforderung initiiert. Wenn der Servlet-Container, der den Scoring-Service auf diesem Rechner ausführt, keine Umkehrsuche im Domain Name System zulässt, entspricht der Wert der IP-Adresse des Computers. Wenn kein Hostname ermittelt werden kann, wird ein Nullwert verwendet. In Fällen, in denen das Nachschlagen des Hostnamens zu lange dauert, ist es möglich, die Leistung des Scoring-Service zu erhöhen, indem das System mithilfe der entsprechenden Konfigurationsoption im browserbasierten IBM® SPSS® Collaboration and Deployment Services Deployment Manager so eingestellt wird, dass es den Hostnamen nicht nachschlägt.

PRINZIPAL. Der Benutzername, der mit der Scoring-Anforderung verknüpft ist. Wenn dieser Wert nicht in der Anforderung enthalten ist, wird keine Information protokolliert.

STAMP. Diese Spalte enthält den Zeitstempel der Zeit, zu der die Anforderung vom Scoring-Service protokolliert wurde.

MODEL_OBJECT_ID. Die Repository-ID des Objekts, das mit dem Scoring-Service konfiguriert wurde. Wenn beispielsweise ein IBM® SPSS® Modeler-Stream für das Scoring konfiguriert wurde, ist das die Repository-ID des Streams.

MODEL_VERSION_MARKER. Der Bezeichner der speziellen Version des Repository-Objekts, das für das Scoring konfiguriert wurde.

CONFIGURATION_NAME Der Name des Konfigurationseintrags des Scoring-Services. Der Name wird zugewiesen, wenn ein Modell für das Scoring konfiguriert wird.

Eingabe für die Scoring-Anforderung (SPSSSCORE_V_LOG_INPUT)

Diese Ansicht enthält die Informationen zu den Modelleingaben, die zur Erstellung des Score verwendet wurden. SPSSSCORE_V_LOG_INPUT kann mehrere Zeilen enthalten, und zwar für jede Zeile in der Tabelle SPSSSCORE_LOG und in der Ansicht SPSSSCORE_V_LOG_HEADER. Jede Zeile in der Ansicht SPSSSCORE_V_LOG_HEADER steht für einen einzelnen Eingabewert.

SERIAL. Die eindeutige ID der Scoring-Anforderungszeile.

INPUT_TABLE. Falls es sich bei der Eingabequelle um IBM® SPSS® Collaboration and Deployment Services Enterprise View handelt, ist dies der Enterprise-Ansicht-Tabellenname.

INPUT_NAME. Der Name eines Eingabefelds. Falls es sich bei der Eingabequelle um Enterprise-Ansicht handelt, ist dies der Enterprise-Ansicht-Spaltenname.

INPUT_VALUE. Der Eingabewert.

INPUT_TYPE. Der Eingabedatentyp. Die folgenden Datentypen sind zulässig:

- Datum
- Tageszeit
- Dezimal
- double
- float
- integer
- long
- String
- timestamp

Kontextdaten der Scoring-Anforderung (SPSSSCORE_V_LOG_CONTEXT_INPUT)

Diese Ansicht enthält die Informationen zu den Daten, die an den Scoring-Service übergeben und als Kontextdatenquelle für die Enterprise-Ansicht Daten-Provider-Definition – Echtzeit verwendet werden. SPSSSCORE_V_LOG_CONTEXT_INPUT kann mehrere Zeilen enthalten, und zwar für jede Zeile in der Ansicht SPSSSCORE_V_LOG_HEADER.

SERIAL. Die eindeutige ID der Scoring-Anforderungszeile.

CONTEXT_TABLE. Der Name der in der Kontextdatenquelle verwendeten Tabelle.

CONTEXT_ROW. Die Zeilennummer der Kontextdatenzeile beginnend mit der Zahl 1.

CONTEXT_NAME. Der Name eines Eingabefelds, der dem Namen der Spalte in der Kontextdatenquelle entspricht.

CONTEXT_VALUE. Der Eingabewert.

Ausgabe der Scoring-Anforderung (SPSSSCORE_V_LOG_OUTPUT)

Die Ansicht SPSSSCORE_V_LOG_OUTPUT wird verwendet, um die Ausgabe des Scoring-Service zu protokollieren. SPSSSCORE_V_LOG_OUTPUT kann für jede Zeile in der Ansicht SPSSSCORE_V_LOG_HEADER mehrere Zeilen enthalten. Der Scoring-Service kann mehrere Ausgaben liefern. Jede Ausgabe kann aus mehreren Werten bestehen. Beispielsweise kann der Scoring-Service zwei Empfehlungen anbieten (zwei Ausgaben). Jeder dieser Empfehlungen wird eine eigene Zeilennummer beginnend mit der Zahl 1 zugewiesen. Für jede Empfehlung können mehrere Ausgabewerte vorhanden sein.

SERIAL. Die eindeutige ID der Scoring-Anforderungszeile.

OUTPUT_ROW. Die Zeilennummer der Kontextdatenzeile beginnend mit der Zahl 1.

OUTPUT_NAME. Der Name des Ausgabefelds (Attribut "Name"), der dem Namen der Spalte in der Kontextdatenquelle entspricht.

OUTPUT_VALUE. Der Ausgabewert.

Maße für die Scoring-Anforderung (SPSSSCORE_V_LOG_METRIC)

Die Ansicht SPSSSCORE_V_LOG_METRIC wird verwendet, um die Ausgabemaße des Scoring-Service zu protokollieren, beispielsweise die zur Verarbeitung einer Scoring-Anforderung benötigte Zeit. SPSSSCORE_V_LOG_METRIC kann für jede Zeile in der Ansicht SPSSSCORE_V_LOG_HEADER mehrere Zeilen enthalten.

SERIAL. Die eindeutige ID der Scoring-Anforderungszeile.

METRIC_NAME. Der Name eines Maßfelds.

METRIC_VALUE. Der Maßwert.

Eigenschaften der Scoring-Anforderung (SPSSSCORE_V_LOG_PROPERTY)

Die Ansicht SPSSSCORE_V_LOG_PROPERTY wird verwendet, um die bei der Verarbeitung der Anforderung verwendeten Eigenschaften zu protokollieren. SPSSSCORE_V_LOG_PROPERTY kann für jede Zeile in der Ansicht SPSSSCORE_V_LOG_PROPERTY mehrere Zeilen enthalten. Die Eigenschaften, die protokolliert werden können, sind vom ausgewählten Score-Anbieter abhängig.

SERIAL. Die eindeutige ID der Scoring-Anforderungszeile.

METRIC_NAME. Der Name einer Eigenschaft.

OUTPUT_VALUE. Der Eigenschaftswert.

Beispiele für Audit-Abfragen

Nachfolgend erhalten Sie Beispiele für SQL-Abfragen in Audit-Ansichten. Beachten Sie, dass bestimmte SQL-Funktionen für Microsoft SQLServer spezifisch und eventuell auf anderen Datenbankplattformen ungültig sind.

Erfolgreiche Anmeldeversuche für Benutzer 'jsmith'

```
select AUDITTIMESTAMP as Login date,
ADDRESS as Machine address
from SPSSPLAT_V_AUDIT
where AUDITCOMPONENT = 'security/componentAuthN'
and AUDITCATEGORY = 'security/locAuthen'
and AUDITTITLE = 'jsmith'
order by 1 desc
```

Erfolgreiche Anmeldeversuche für alle Benutzer

```
select AUDITTITLE as Username,
AUDITTIMESTAMP as Login date,
ADDRESS as Machine address
from
SPSSPLAT_V_AUDIT
where AUDITCOMPONENT = 'security/componentAuthN'
and AUDITCATEGORY = 'security/locNotAuthen'
order by 1 asc, 2 desc
```

Anzahl erfolgreicher Anmeldeversuche für jeden Benutzer im letzten Monat

```
select AUDITTITLE as Username,
COUNT(*) as Successful logins
from
SPSSPLAT_V_AUDIT
where AUDITCOMPONENT = 'security/componentAuthN'
and AUDITCATEGORY = 'security/locAuthen'
and AUDITTIMESTAMP >= DATEADD(month, -1, GETDATE())
group by AUDITTITLE
order by 2 desc
```

Alle Repository-Ressourcen mit der benutzerdefinierten Eigenschaft "Region"

```
select V1.FILEPATH + V1.FILENAME as Resource, V2.PROPERTYNAME + ' = ' + V2.PROPERTYVALUE as Property/Value
from SPSSPLAT_V_FILEINFO V1,
SPSSPLAT_V_CUSTOMPROPERTY V2
where V1.FILEID = V2.FILEID
and V2.PROPERTYNAME = 'Region'
```

Alle Repository-Ressourcen mit dem benutzerdefinierten Eigenschaftswert "Asiatisch-Pazifisch"

```
select V1.FILEPATH + V1.FILENAME as Resource, V2.PROPERTYNAME + ' = ' + V2.PROPERTYVALUE as Property/Value
from SPSSPLAT_V_FILEINFO V1,
SPSSPLAT_V_CUSTOMPROPERTY V2
```

```
where V1.FILEID = V2.FILEID  
and V2.PROPERTYVALUE = 'Asiatisch-Pazifisch'
```

Alle geänderten Repository-Ressourcen (neu erstellte Versionen) von Benutzer 'jsmith'

```
select FILEPATH + '/' + FILENAME as Resource,  
VERSION as Version,  
VERSIONCREATEDDATE as Modified date  
from SPSSPLAT_V_FILEVERSION  
where VERSIONCREATEDBY = 'jsmith'
```

Alle Benutzer, die die Datei /Modeler/Base_Module/drugplot.str geändert haben

```
select VERSION as Version,  
VERSIONCREATEDBY as Username,  
VERSIONCREATEDDATE as Created date  
from SPSSPLAT_V_FILEVERSION  
where FILEPATH + FILENAME = '/Modeler/Base_Module/drugplot'
```

Fehlerbehebung

Bestimmte Fehlermeldungen und Symptome treten bei der Installation des IBM® SPSS® Collaboration and Deployment Services Repository und bei der Arbeit damit häufig auf. Methoden zur Behebung dieser Fehler und zur Einrichtung eines funktionierenden Systems existieren für:

- **Das Repository.** Häufig auftretende Probleme bei der Installation und beim Starten der Anwendung auf unterstützten Server-Plattformen.
- **Solaris 9.** Bekannte Probleme in Verbindung mit dem Repository auf dem UNIX-Betriebssystem von Sun.
- **HP-UX.** Bekannte Probleme in Verbindung mit dem Repository auf dem UNIX-Betriebssystem von HP.
- **DB2 für IBM i.** Symptome und Fehlermeldungen, die bei Transaktionen mit einer auf IBM i ausgeführten DB2-Datenbank auftreten.
- **Oracle 10g und 11g.** Symptome und Fehlermeldungen, die bei Transaktionen mit Oracle 10g- und 11g-Datenbanken auftreten.
- **JBoss.** JBoss-Anwendungsserver, auf dem das Repository ausgeführt wird.
- **Oracle WebLogic.** WebLogic-Anwendungsserver, auf dem das Repository ausgeführt wird.
- **WebSphere.** WebSphere-Anwendungsserver, auf dem das Repository ausgeführt wird.

Es ist immer sinnvoll, die Repository-Protokolldateien einzusehen, um die Ursache des Problems zu finden.

Fehlerbehebung beim Repository

Wie vermeide ich beim Start und beim Einsatz des Repository Leistungsengpässe und Probleme hinsichtlich der CPU-Belastung?

Abhängig von der spezifischen Systemkonfiguration könnte es sein, dass zuvor installierte Antivirus- oder Spyware-Software für "Tiefenscans" von Anwendungskomponenten konfiguriert ist. Solche Anwendungen von Drittanbietern können neu konfiguriert werden, sodass Sie nur zu bestimmten Zeiten Scans durchführen, oder sie können während der Installation deaktiviert und später erneut manuell gestartet werden.

Außerdem können sich einige der strengeren serverseitigen Firewall-Einstellungen negativ auf die Startgeschwindigkeit auswirken und den Zugriff unterbinden.

Wenn Sie beim Starten des Dienstes einen erheblichen Abfall der Systemleistung beobachten, deaktivieren Sie alle unnötigen Prozesse und starten Sie das Repository erneut.

Wie kann ich während der Anmeldung bei der Administratoroberfläche bestimmen, auf welche Datenbank ich zugreife?

Datenbankverbindungsinformationen können aus der Weboberfläche heruntergeladen werden und Sie können von dort aus auf sie zugreifen.

1. Klicken Sie nach der Authentifizierung auf Info über in den Navigationslistenoptionen. Die Seite "Info über" wird angezeigt.
2. Klicken Sie auf den Link Version und Systemdaten herunterladen am unteren Rand der Seite. Speichern Sie die Datei auf der Festplatte, wenn Sie dazu aufgefordert werden.
3. Öffnen Sie die Datei in einem Texteditor und suchen Sie nach *Database Details*. Dieser Abschnitt enthält detaillierte Informationen zu der verwendeten Datenbank, darunter Name, Version und eine Tabellenauflistung.

Die Anwendung gibt die Fehlermeldung `java.lang.OutOfMemoryError: PermGen space exception`.

Dieser Fehler tritt auf, wenn der Speicher für die JVM im Permanent Generation Heap aufgrund einer großen Anzahl verwendeter Klassen knapp wird. Der Fehler kann bei der Ausführung von IBM® SPSS® Collaboration and Deployment Services oder der zugehörigen Dienstprogramme, wie dem Setup-Pogramm, dem Speicher- und Wiederherstellungsprogramm oder dem Package Manager, auftreten. Je nach Speicherkonfiguration des Systems kann die Lösung darin bestehen, den in den Startskripts von Anwendungsserver und Dienstprogrammen für den Parameter "PermSize JVM" festgesetzten Wert zu erhöhen bzw. herabzusetzen. Wenn der Gesamtverbrauch an Arbeitsspeicher durch Anwendungsserver und Dienstprogramme wesentlich kleiner ist als der freie Arbeitsspeicher des Systems und ein Ausnahmefehler wegen Speichermangels auftritt, sollten Sie den Wert erhöhen. Wenn der Gesamtverbrauch an Arbeitsspeicher durch Dienstprogramme und Anwendungsserver größer ist als der freie Arbeitsspeicher des Systems, sollten Sie versuchen, die Größe des Permanent Generation Heap zu verringern.

Bei JBoss-Installationen z. B. kann die Größe des Permanent Generation Heap, die dem Wrapper-Service zur Verfügung steht, ab der folgenden Stelle geändert werden:

```
<JBoss-Installationsverzeichnis>/wrapper/conf/wrapper.conf:
```

```
wrapper.java.additional.1=-Dprogram.name=run.bat -XX:PermSize=128m.
```

Informationen zur Erhöhung der Permanent Generation Heap-Größe für andere Anwendungsserver finden Sie in der Herstellerdokumentation des Anwendungsservers.

Wenn während der Ausführung der Dienstprogramme ein Speicherfehler auftritt, müssen Sie die Startskripts für diese Dienstprogramme ändern, um niedrigere Werte für die JVM-Arbeitsspeicherparameter festzulegen. Beispielsweise lautet der Java-Befehl in `packagemanager.sh/packagemanager.bat` wie folgt:

```
java -Xms128m -Xmx1024m -XX:PermSize=512m -classpath $CP com.spss.setup.packagemanager.ui.PlatformPackageTool $@
```

Er kann geändert werden in:

```
java -Xms128m -Xmx512m -XX:PermSize=256m -classpath $CP com.spss.setup.packagemanager.ui.PlatformPackageTool $@
```

Fehler über Speichermangel können auch durch Hinzufügen von JVM-Parametern zur Feinabstimmung von Speicherzuteilung und Datenentsorgung vermieden werden, z. B.:

-XX:+CMSPermGenSweepingEnabled -XX:+CMSClassUnloadingEnabled

Wenn ein BIRT Report Designer for IBM SPSS-Bericht in IBM SPSS Collaboration and Deployment Services Deployment Portal ausgeführt wird, kann die Anwendung meine Anmeldeinformationen für den Zugriff auf die Datenquelle des Berichts nicht authentifizieren, sodass immer wieder das Anmeldefenster angezeigt wird.

- Stellen Sie sicher, dass die Datenquelle für den Bericht und die Anmeldeinformationen korrekt definiert sind. Weitere Informationen finden Sie im entsprechenden Abschnitt des *IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Benutzerhandbuchs*.
- Falls die Datenquelle für den Bericht JDBC-basiert ist, stellen Sie sicher, dass der richtige Treiber zusammen mit dem Repository installiert wurde. Informationen zu für die Betriebsplattform spezifischen Treiberpfaden finden Sie in den Installationsanweisungen.

Ein SAS-Syntaxjob, der im Repository auf einem UNIX-System verarbeitet wird, schlägt fehl, wobei ein Datenbankverbindungsfehler aufgrund eines ungültigen Bibliotheksnamens gemeldet wird ("ERROR: Error in the LIBNAME statement").

- Stellen Sie sicher, dass die Umgebungsvariable für den Pfad der freigegebenen Bibliotheken (LD_LIBRARY_PATH unter Solaris, SHLIB_PATH unter HP-UX oder LIBPATH unter AIX) auf einen entsprechenden Wert eingestellt ist.

Wie stelle ich das Repository wieder her, wenn meine Schlüsselspeicher-Datei verloren gegangen ist?

Die Schlüsselspeicher-Datei enthält die Schlüssel, die zur Verschlüsselung der vom Repository verwendeten Passwörter verwendet werden, beispielsweise das Master-Passwort für den Datenbankzugriff. Falls die Schlüsselspeicher-Datei verloren geht, kann das System nicht mehr verwendet werden. Falls eine Sicherungskopie der Schlüsselspeicher-Datei vorhanden ist, kann sie am ursprünglichen Speicherort wiederhergestellt werden. Wenn Sie sich nicht sicher sind, unter welchem Pfad die Schlüsselspeicher-Datei ursprünglich gespeichert war, können Sie die Eigenschaft *keystorePath* des Elements *keystoreSecurity* unter *<Repository-Installationsverzeichnis>/platform/setupinfo.xml* einsehen.

Wenn die Schlüsselspeicher-Datei verloren gegangen und keine Sicherungskopie vorhanden ist, muss das System durch erneute Ausführung des Setup-Dienstprogramms unter *<Repository-Installationsverzeichnis>/setup* neu installiert und ein Verweis auf die vorhandene Repository-Datenbank angegeben werden. Alle Passwörter des Systems wie z. B. Passwörter für externe Verzeichnisdienste, definierte Anmeldeinformationen usw. müssen manuell erneut eingegeben werden.

Ein BIRT-Bericht über eine DB2 IBM i V6R1-Datenbank mit angeforderten Anmeldeinformationen schlägt bei der Ausführung im Repository fehl.

Fügen Sie den Parameter *prompt=true* zur URL der JDBC-Verbindung hinzu.

Treibername: com.ibm.as400.access.AS400JDBCdriver
 Driver URL: jdbc:as400://myServer/B101E31E;prompt=false

Die Fehlermeldung "Erstellen neuer Scoring-Konfigurationsdetails fehlgeschlagen" wird angezeigt, wenn das Scoring auf Repository-Installationen unter einem anderen Betriebssystem als Windows konfiguriert wird.

Die Fehlermeldung "Erstellen neuer Scoring-Konfigurationsdetails fehlgeschlagen" wird angezeigt, wenn das Dialogfeld "Scoring-Konfiguration" in Deployment Manager geöffnet wird. Das Problem kann behoben werden, indem die Berechtigungen der Datei in `<Repository-Installationsverzeichnis>/components/modeler/modelerserver` auf `execute` geändert werden, z. B.:

```
cd /usr/CDS/components/modeler/modelerserver
sudo chmod +x modelerserver
```

Berichtsausgaben, die als PDF-Datei generiert werden, zeigen nationale Zeichensätze nicht korrekt an.

Auf bestimmten UNIX-Systemen ist die standardmäßige JVM-Schriftkonfiguration möglicherweise nicht für alle nationalen Zeichensätze geeignet, z. B. für Schriftzeichen in asiatischen Sprachen. In diesen Fällen kann es erforderlich sein, die JVM-Standardschrift mithilfe einer Schriftkonfigurationsdatei anzugeben. Weitere Informationen zu Java-Schriftkonfigurationsdateien finden Sie in der Sun-Dokumentation.

Solaris

Das Repository kann auf JBoss und Solaris 9 nicht gestartet werden.

Beim Versuch, das Repository auf JBoss und Solaris 9 zu starten, wird die Fehlermeldung `"ld.so.1: wrapper: fatal: libm.so.2 open failed: No such file.."` angezeigt.

Erstellen Sie zur Lösung dieses Problems die symbolische Verknüpfung `/usr/lib/64/libm.so.2` zu `/usr/lib/64/libm.so.1`:

```
ln -s /usr/lib/64/libm.so.1 /usr/lib/64/libm.so.2
```

HP-UX

Importfehler bei der Ausführung des Repository unter HP-UX mit NFS.

Bei Ausführung unter HP-UX mit NFS kann beim Importieren von Ressourcen in das Repository folgende Ausnahme auftreten:

```
java.lang.RuntimeException: The database is already in use by another process: org.hsqldb.persist.NIOLockFile@3ffdc36b[file
=/qa/projects/pes/HPUX/appserv/boa11g/user_projects/domains/Domain41B179a/cds_transfer_root/
0a0b0ad397fef2c500000126b4ca991881ab/0a0b0ad397fef2c500000126b4ca991881ad_transfer_database.lck,
exists=true, locked=false, valid=false, fl=null]:
```


Legen Sie zur Lösung des Problems mithilfe des browserbasierten IBM® SPSS® Collaboration and Deployment Services Deployment Manager für die Konfigurationsoption *Repository* -> *Nachschlagetabelle für Ressourcenübertragung* den Wert MEMORY fest. Weitere Informationen finden Sie in der IBM® SPSS® Collaboration and Deployment Services-Administratordokumentation.

Oracle-Datenbank

Wie erstelle ich einen Benutzer und einen Tablespace?

Um den *spssplat*-Benutzer und -Tablespace aus einer Oracle-Datenbank zu entfernen und neu zu definieren, führen Sie folgende Befehlsfolge aus:

```
drop user spssplat cascade; CREATE USER spssplat IDENTIFIED BY spssplat
DEFAULT TABLESPACE SPSSPLAT TEMPORARY TABLESPACE TEMP
QUOTA UNLIMITED ON SPSSPLAT;
@$ORACLE_HOME/sqlplus/admin/pupbld;
GRANT CONNECT, RESOURCE, UNLIMITED TABLESPACE TO spssplat;
```

JBoss

Wie konfiguriert man den Zeitbeschränkungswert für Sitzungen, um einzustellen, wie lang ein Benutzer inaktiv bleiben kann?

Wenn ein Benutzer beim Repository angemeldet ist, ist ein bestimmter Inaktivitätszeitraum erlaubt, bevor die Sitzung beendet wird und der Benutzer erneut authentifiziert werden muss. So erhöhen oder verringern Sie diesen Wert:

1. Navigieren Sie vom Installationsverzeichnis aus nach
`\JBoss\server\default\deploy\jbossweb-tomcat50.sar\`.
2. Öffnen Sie *web.xml* in einem Texteditor.
3. Finden Sie den Abschnitt für *Default Session Configuration* und bearbeiten Sie den Wert für `<session-timeout>`.
4. Beenden Sie die Anwendung und starten Sie sie erneut.

Hinweis: Diese Datei wird verarbeitet, wenn die Anwendung eingesetzt wird; Änderungen an der Konfiguration werden erst wirksam, wenn der Server neu gestartet wird.

Wie kann ich den Port festlegen, über den meine Version von JBoss ausgeführt wird?

Der HTTP-Port des JBoss-Anwendungsservers ist in folgender Datei definiert:

```
jboss-3.2.7\server\default\deploy\jbossweb-tomcat50.sar\server.xml
```

mit dem Attribut:

/Server/Service/Connector@port

Hinweis: Abhängig von der Version von JBoss können die Versionsnummern im Pfad abweichen.

Welche zusätzlichen Einstellungen sind für FIPS 140-2-Konformität des Repository auf JBoss erforderlich?

Damit das Repository bei der Ausführung auf JBoss in FIPS 140-2-konformem Modus einwandfrei funktioniert, muss das Attribut {URIEncoding=UTF-8} für die HTTPS-Verbindung angegeben werden.

Alternativ kann aus der Befehlszeile der netstat-Befehl ausgeführt werden, um Anwendungen und die verwendeten Ports anzuzeigen.

WebLogic

“IOException: Resource has been deleted” wird in IBM SPSS Collaboration and Deployment Services Deployment Portal gemeldet, wenn versucht wird, auf Dateianhänge zuzugreifen, die Berichtsangaben enthalten.

Dieser Ausnahmefehler kann auftreten, wenn die Repository-Installation auf einem WebLogic-Anwendungsserver ausgeführt wird, der JRockit anstelle von Sun JRE verwendet. Falls dieser Ausnahmefehler auftritt, konfigurieren Sie WebLogic neu, sodass es Sun JRE verwendet. Weitere Informationen finden Sie in der WebLogic-Dokumentation.

Kaskadierende Parameter werden in Berichten nicht korrekt angezeigt, wenn das Repository mit WebLogic 10 auf Solaris 10 ausgeführt wird.

Das Start-Argument -Djava.awt.headless=true muss der Java-Umgebung des Anwendungsservers hinzugefügt werden.

Repository-Setup auf Red Hat v5.4 schlägt fehl mit der Meldung, dass zu viele Dateien geöffnet sind.

Dieser Fehler wird generiert, wenn die maximale Anzahl geöffneter Dateien für einen Benutzer die Standardeinstellung überschreitet. Sie können mithilfe des folgenden Befehls diese Einstellung überprüfen:

```
ulimit -n
```

Das Limit der geöffneten Dateien des Benutzers lässt sich durch Bearbeiten der Datei */etc/security/limits.conf* erhöhen, indem beispielsweise die folgende Zeile angefügt wird:

```
@username - nofile 2048
```

Das System muss dann neu gestartet werden, damit der neue Grenzwert wirksam wird.

Benachrichtigungsmeldungen werden nicht an den RSS-Reader ausgegeben.

Der Fehler wird durch ein Versagen der HTTP-Basisauthentifizierung auf der Domänenebene verursacht. Er lässt sich durch Deaktivieren der HTTP-Basisauthentifizierung für die Domäne beheben. Fügen Sie das Element `<enforce-valid-basic-auth-credentials>` zur `config.xml`-Datei der Domäne im `<security-configuration>`-Element hinzu und setzen sie seinen Wert auf `false`.

```
...
<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>

</security-configuration>
```

WebSphere

Verschiedene Fehler treten während einer Paketinstallation (mit Package Manager) im Repository unter Verwendung eines WebSphere-Anwendungsservers auf.

Stellen Sie sicher, dass die aktuellen Hersteller-Patches auf dem Anwendungsserver installiert wurden.

Das Serverprotokoll meldet Verschlüsselungsfehler, z. B. den Ausnahmefehler "com.ibm.crypto.provider.AESCipher.engineGetKeySize(Unknown Source)"

Der Fehler tritt mit WebSphere 6.1 Service-Pack 19 auf und wird durch den fehlerhaften Passwortwert verursacht. Kopieren Sie zur Korrektur des Fehlers den Wert von `platform.keystore.password` aus

```
<Repository-Installationsverzeichnis>/platform/setupinfo.xml
```

nach

```
<WEBSphere_HOME>/profiles/AppSrv01/config/cells/xi-wyueNode01Cell/nodes/xi-wyueNode01/servers/
<Servername>/server.xml
```

Ein Upgrade auf WebSphere 6.1 Service-Pack 23 kann auch Verschlüsselungsprobleme beseitigen.

"CWSIS1535E: Die eindeutige ID der Messaging-Engine entspricht nicht derjenigen, die im Datastore-Fehler angegeben ist.

Der Fehler lässt sich durch Stoppen des Repository und Löschen der Repository-Datenbanktabellen beseitigen, deren Namen mit dem Präfix `SIB` beginnen. Beim Neustart des Repository werden die Tabellen erneut angelegt. Beachten Sie, dass diese Lösung nur sinnvoll ist, wenn Sie keine der aktuell gespeicherten persistenten Meldungen aufbewahren müssen. Weitere Informationen über die WebSphere JMS-Fehlerbehebung finden Sie unter <http://www.redbooks.ibm.com/redpapers/pdfs/redp4076.pdf>.

Remote-Ausnahmefehler bei der Ausführung eines BIRT-Berichts bei einer IBM SPSS Statistics-Datenquelle (mit IBM SPSS Statistics-Datendatei-JDBC-Treiber) in einem WebSphere-Cluster

Das Problem kann dadurch Hinzufügen von `Dcom.ibm.ws.classloader.encodeResourceURLs=true` zu den generischen JVM-Argumenten gelöst werden, wobei die WebSphere-Administrationskonsole für jeden Knoten im Cluster verwendet wird.

Beim Durchführen einer Installations- oder Einrichtungsaktion schlägt die Aktion fehl und das Protokoll verweist darauf, dass auf mindestens eine systemeigene Bibliotheksdatei (.dll, .so, .sl) nicht zugegriffen werden konnte.

Dieses Problem tritt in der Regel auf, wenn versucht wird, die systemeigenen Bibliotheken in einem Scoring-Provider-Paket zu aktualisieren, während eine Scoring-Konfiguration aktiv ist und die aktuellen Bibliotheken verwendet. Dies kann in den folgenden Situationen der Fall sein:

- IBM® SPSS® Collaboration and Deployment Services Package Manager wird zum Installieren eines Scoring-Adapters in einem Repository verwendet, in dem bereits eine Version dieses Scoring-Adapters installiert ist.
- Ein Patch mit einem Scoring-Adapter wird in einem System angewendet, in dem bereits eine Version dieses Scoring-Adapters installiert ist.
- Erneutes Ausführen des IBM® SPSS® Collaboration and Deployment Services Setup auf einem Repository der Version 4.0 oder höher, wenn in diesem Repository bereits ein Scoring-Adapter installiert wurde. Dies erstreckt sich auch auf das erneute Ausführen des Setup-Tool nach dem Wiederherstellen.

Stellen Sie vor der Installations- oder Einrichtungsaktion sicher, dass diese Scoring-Bibliotheken nicht ausgeführt werden, um dieses Problem zu vermeiden. Die grundlegenden Schritte hierfür gestalten sich wie folgt:

1. Starten Sie die WebSphere-Administrationskonsole und navigieren Sie zu den bereitgestellten Anwendungen für Ihren Repository-Server.
2. Deaktivieren Sie die Option zum automatischen Starten für die Anwendungen *scoring* und *scoring-ejb*.
3. Wenn das Repository in Version 4.0 oder höher vorliegt, deaktivieren Sie die Option zum automatischen Starten für die Anwendungen *admin*, *security* und *security-ws*.
4. Speichern Sie die Änderungen und starten Sie den WebSphere-Anwendungsserver neu.
5. Führen Sie die gewünschte Installations- oder Einrichtungsaktion durch.
6. Wechseln Sie wieder zur WebSphere-Administrationskonsole und aktivieren Sie die Option zum automatischen Starten für die zuvor deaktivierten Anwendungen.
7. Speichern Sie die Änderungen und starten Sie den WebSphere-Anwendungsserver neu.

Nativestore-Schema-Referenz

Das *nativestore.xsd*-Schema definiert die Struktur einer XML-Datei, die Benutzer und Gruppen enthält, die in der Deployment Manager importiert werden sollen. Zusätzlich kann die Datei veraltete Benutzer und Gruppen angeben, die gelöscht werden sollen.

Beispiel XML

```
<?xml version=1.0 encoding=UTF-8?>
<nativestore>
  <user userID=sbennett password=sb9482 encrypted=false>
    <group>sales</group>
  </user>
  <user userID=lsanborn password=ls7725 encrypted=false>
    <group>sales</group>
  </user>
  <user userID=larger password=la4011 encrypted=false>
    <group>analyst</group>
  </user>
  <user userID=cjones password=cj2683 encrypted=false>
    <group>analyst</group>
  </user>
  <obsolete>
    <user>mmonroe</user>
    <user>bgmurphy</user>
    <group>jones project</group>
  </obsolete>
</nativestore>
```

nativestore-Element

Untergeordnete Elemente: [user](#), [obsolete](#)

Stammelement für den Import von lokalen Benutzern und ihren Gruppen in der Deployment Manager.

user-Element

Übergeordnetes Element: [nativestore](#)

Untergeordnete Elemente: [group](#), [role](#)

Benutzer wird hinzugefügt oder aktualisiert.

Tabelle B-1

Attribute für das `user-Element`

Name	Typ	Verwenden	Standard	Beschreibung
userID	String	erforderlich	kein Standardwert	Benutzer-ID, die für die Anmeldung beim System verwendet wird.
password	String	optional	kein Standardwert	Für gewöhnlich ein Standardtext-Passwort. Wenn das <code>encrypted</code> -Attribut auf "wahr" gestellt ist, wird dieses Passwort verschlüsselt. Für gewöhnlich ist es nicht möglich, beim Import ein verschlüsseltes Passwort zu verwenden. Passwörter werden beim Export vom Server verschlüsselt, dies wird jedoch <i>nicht</i> in der Deployment Manager-Benutzeroberfläche dargestellt.
verschlüsselt	boolean	optional	false	Zeigt an, ob das Passwort Standardtext oder verschlüsselt ist. Verschlüsselte Passwörter werden aus dem Native Store exportiert (dies ist eine Einweg-Verschlüsselung, die eine Wiederherstellung eines Benutzerpassworts unmöglich macht). Beim Import aus einem anderen System müssen Passwörter in Standardtext gehalten sein; das <code>encrypted</code> -Attribut wird für gewöhnlich weggelassen.

Beispiel XML

```
<?xml version=1.0 encoding=UTF-8?>
<nativestore>
  <user userID=sbennett password=sb9482 encrypted=false>
    <group>sales</group>
  </user>
</nativestore>
```

group-Element

Typ: Zeichenkette

Übergeordnetes Element: [user](#)

Gruppen, die mit dem Benutzer verknüpft sind. Falls eine Gruppe nicht vorhanden ist, wird sie automatisch erstellt.

Beispiel XML

```
<?xml version=1.0 encoding=UTF-8?>
<nativestore>
  <user userID=sbennett password=sb9482 encrypted=false>
    <group>sales</group>
```

```
</user>  
</nativestore>
```

role-Element

Typ: Zeichenkette

Übergeordnetes Element: [user](#)

Rolle, die mit dem Benutzer verknüpft ist. Falls eine Rolle nicht vorhanden ist, wird sie *nicht* automatisch hinzugefügt.

obsolete-Element

Übergeordnetes Element: [nativestore](#)

Untergeordnete Elemente: [user](#), [group](#)

Gruppen oder Benutzer, die entfernt werden sollen. Beachten Sie, dass sie im “Ersetzen-Modus” geladen werden können, der automatisch alle Gruppen und nicht administrativen Benutzer entfernt. In diesem Modus hat dieses Element keine Wirkung.

Beispiel XML

```
<?xml version=1.0 encoding=UTF-8?>  
<nativestore>  
  <obsolete>  
    <user>mmonroe</user>  
    <user>bgmurphy</user>  
    <group>jones project</group>  
  </obsolete>  
</nativestore>
```

user-Element

Typ: Zeichenkette

Übergeordnetes Element: [obsolete](#)

Die Benutzer-ID, die entfernt werden soll. Benutzer mit Administratorberechtigungen können nicht entfernt werden.

Beispiel XML

```
<?xml version=1.0 encoding=UTF-8?>  
<nativestore>  
  <obsolete>  
    <user>mmonroe</user>  
  </obsolete>  
</nativestore>
```

group-Element

Typ: Zeichenkette

Übergeordnetes Element: [obsolete](#)

Gruppenname, der entfernt werden soll.

Beispiel XML

```
<?xml version=1.0 encoding=UTF-8?>
<nativestore>
  <obsolete>
    <group>jones project</group>
  </obsolete>
</nativestore>
```


Notices

Licensed Materials – Property of SPSS Inc., an IBM Company. © Copyright SPSS Inc. 2004, 2010..

Patent No. 7,023,453

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: SPSS INC., AN IBM COMPANY, PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. SPSS Inc. may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-SPSS and non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this SPSS Inc. product and use of those Web sites is at your own risk.

When you send information to IBM or SPSS, you grant IBM and SPSS a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Information concerning non-SPSS products was obtained from the suppliers of those products, their published announcements or other publicly available sources. SPSS has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-SPSS products. Questions on the capabilities of non-SPSS products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to SPSS Inc., for the purposes of developing,

using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. SPSS Inc., therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided “AS IS”, without warranty of any kind. SPSS Inc. shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks of IBM Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>.

SPSS is a trademark of SPSS Inc., an IBM Company, registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other product and service names might be trademarks of IBM, SPSS, or other companies.

Adobe product screenshot(s) reprinted with permission from Adobe Systems Incorporated.

Microsoft product screenshot(s) reprinted with permission from Microsoft Corporation.



- Abfragebeispiele, 131
- Abmeldung, 9
- Abonnement-ID-Cache, 105
- Abonnementverwaltung, 107
- Abstimmen der Leistung, 105
- Active Directory, 25, 48, 56
 - Aktivieren, 50
 - Deaktivieren, 50
 - mit lokaler Überschreibung, 48, 51, 57
- Active Directory mit lokaler Überschreibung, 25–26
- Administratoren, 42
- Administratorrechte, 62–63, 68, 70
- Aktionen, 25–26
 - Entfernen aus Rollen, 45
 - Hinzufügen zu Rollen, 45
 - Rollen, 40
- ändern
 - Passwörter, 14
- Ändern
 - Benutzer, 31
 - groups, 34
- Angeforderte Anmeldeinformationen, 135
- Anmeldeinformationen, 65
- Anmelden, 9
- Anmeldungen
 - Caching, 84
- Anmeldungsseite, 13–14
- Anpassen
 - Benachrichtigungen, 96, 98
 - Benachrichtigungsmeldungen, 95, 100
 - Meldungsvorlagen, 95, 100
- Anzeigen
 - Job-Ausgabe, 105
 - Server-Eigenschaften, 21
- Apache ActiveMQ, 111
- Asiatische Sprachen, 136
- Audit-Abfragen, 131
- Audit-Ansichten, 116
- Audit-Berichte, 116
- Audit-Tabellen, 116
- Auditing, 110, 116
 - Datenbankschema, 118
 - Ereignisse, 117
- Ausführungsserver, 6
 - Remote-Verarbeitung, 6
 - SAS, 6
- BEA WebLogic, 111
- bearbeiten
 - Benutzer, 31
 - groups, 34
- MIME-Typen, 91
- Rollen, 45
- Beispiel für JMS-Thema-Konfigurationsdatei, 111
- Beispiel für meldungsbasierte Verarbeitung, 114
- Beispiel-Stapeldatei für die Ausführung von JMS-Client, 114
- Benachrichtigung
 - Konfiguration, 70
- Benachrichtigungen, 95
 - Anpassen, 96, 98, 100
 - Betreffstitel, 95
 - Formatierung, 100
 - HTML, 101
 - Inhalt, 95
 - Text, 101
 - Velocity, 95
 - Vorlagen, 95, 102
- Benachrichtigungen, Konfigurationsoptionen, 105
- Benachrichtigungsleistung, Empfehlungen, 105
 - Abonnementverwaltung, 107
 - Anzahl der Abonnements, 107
 - Anzahl der benutzerdefinierten Vorlagen, 107
 - Anzahl der Empfänger, 107
- Benutzer
 - Ändern, 26, 31
 - bearbeiten, 26, 31
 - Einrichten, 26
 - Erlaubt, 25–26, 38
 - erstellen, 26, 29
 - Gruppenmitgliedschaft, 25–26
 - hinzufügen, 26, 29
 - Importieren, 36
 - in IBM SPSS Collaboration and Deployment Services
 - Deployment Manager verwalten, 25–26
 - Lokal, 25–26
 - löschen, 33
 - Remote definiert, 25–26
 - Zugriff auf Systemressourcen, 25–26
- Benutzerdefinierte Dialogfelder, 65
- Benutzerdefinierte Funktionen, 87
- Benutzervoreinstellungen, 4
- Berichtsausgabe, 136
- Berichte, 63
- Betriebssysteme
 - Fehlerbehebung, 136
- Bewertung, 136
- Bilder
 - Zuordnung zu Dateien, 91–92
- BIRT, 63
- BIRT Report Designer for IBM SPSS, 3, 6
- BIRT-Berichtverarbeitung, 135

- Cache, 64
- Caching
 - Anmeldungen, 84
- Cascading Stylesheets, 63
- Coherence, 64
- CWSIS1535E-Fehler, 139

- Dateiberechtigungen, 136
- Dateien
 - Benennen, 23
 - Zuordnung zu Bildern, 91–92
- Datenbank-Auditing, 116
- Datenbanken
 - Fehlerbehebung, 137
- Datenbankschema
 - Auditing, 118
- Datenbanksperre-Ausnahme, 136
- Datenentsorgung, 134
- Datenservice
 - Konfiguration, 66
- DB2, 135
- Deaktivieren von binärem Inhalt , 105
- Debug-Information, 79
- Dedizierter SMTP-Server, 105
- Delivery Status Notifications, 109
- Deployment, 2
- Deployment Manager
 - Konfiguration, 67
- Deployment Portal
 - Konfiguration, 67
- Deployment Portal-Scoring-Konfigurationen, 68
- Domäne, 60
- DSN, 109

- E-Mail-Benachrichtigungen, 95
 - HTML, 101
 - Text, 101
- Eigenschaft "JobStatusURL"
 - in Benachrichtigungsvorlagen, 103
- EIM, 48, 57
- eim.jar, 48
- Einhaltung von Bestimmungen, 116
- Einzelanmeldung, 13, 48, 57, 60
- Einzelplatzlizenz, 16
- encrypted-Attribut
 - für user, 142
- Enterprise Identity Management, 48, 57
- Enterprise-Ansicht, 68
- entfernen
 - MIME-Typen, 92
- Ereignisfilter, 105
- Ereignissammlungspool, 105
- Ereignisse
 - Auditing, 117
 - Job-Ausführung, 117
 - Repository, 117
 - Sicherheit, 117
- Erfassen von Audit-Ereignissen, 117
- Erlaubte Benutzer, 25–26, 38
 - für Active Directory, 51
- Erneute Setup-Durchführung, 135
- erstellen
 - Benutzer, 29
 - Erlaubte Benutzer, 38
 - Erweiterte Gruppen, 37
 - groups, 33
 - Rollen, 43
- Erweiterte Gruppen, 25–26, 37
 - für Active Directory, 51
- exportieren, 42
- Externer Sicherheits-Provider, 26
 - Active Directory, 25
 - Active Directory mit lokaler Überschreibung, 25
 - OpenLDAP, 25

- fehlende JDBC-Treiber, 135
- Fehler, 133, 136–137
 - Diagnose, 133, 136–137
 - Generation Heap-Größe, 133
 - Installation, 133
 - java.lang.OutOfMemoryError: PermGen-Speicher, 133
 - Lösen, 133, 136–137
 - Speicherfehler, 133
 - Wrapper-Service, 133
 - Zugriff, 136
- Fehlerbehebung, 16, 133, 136–137
 - Fehlgeschlagene Benachrichtigungszustellung, 110
- Fehlerdiagnose, 133, 136–137
- Fehlermeldungen, 133, 136–137
- Fehlersuche im Benachrichtigungsdienst, 109
- Fehlgeschlagene Benachrichtigungszustellung, 110
- FIPS 140-2
 - JBoss-Konfiguration, 138
- Freigegebene Bibliotheken, 135

- Generation Heap-Größe, 133
- group-Element
 - in obsolete, 143–144
 - in user, 141–142
- groups
 - Ändern, 26, 34
 - bearbeiten, 26, 34
 - erstellen, 26, 33
 - Erweitert, 25–26, 37
 - hinzufügen, 26, 33
 - Importieren, 36
 - in IBM SPSS Collaboration and Deployment Services
 - Deployment Manager verwalten, 25–26
 - Lokal, 26
 - löschen, 36

- Heap-Größe , 134
- Hilfe, 62, 70

- hinzufügen
 - Benutzer, 29
 - groups, 33
 - MIME-Typen, 90
 - Verwaltete Server, 18
- HP-UX, 136
- IBM i, 135
- IBM i-Benutzer-Repository, 48
- IBM ShowCase Warehouse Builder
 - Konfiguration, 86
- IBM SPSS Collaboration and Deployment Services
 - Deployment Manager, 3–4
- IBM SPSS Collaboration and Deployment Services
 - Deployment Portal, 3–4
- IBM SPSS Collaboration and Deployment Services
 - Enterprise View, 3, 5
- IBM SPSS Collaboration and Deployment Services
 - Package Manager, 140
- IBM SPSS Collaboration and Deployment Services
 - Repository, 3–4
- IBM SPSS Collaboration and Deployment Services
 - Repository-Server
 - Eigenschaften, 21
- IBM SPSS Collaboration and Deployment Services Setup, 140
- IBM SPSS Modeler, 7
- IBM SPSS Modeler-Adapter, 136
- IBM SPSS Modeler-Adapterdateiberechtigungen, 136
- IBM SPSS Statistics
 - Anmeldeinformationen, 65
 - Benutzerdefinierte Dialogfelder, 65
 - Server, 65
- IBM SPSS Statistics-JDBC-Treiber, 140
- Importfehler, 136
- Importieren, 42
- Importieren von Benutzern und Gruppen, 36
- Indexerstellung
 - Bei Repository-Upgrade, 93
 - Berechtigung für Ausführung, 93
 - Konfigurationsoption für Erzwingung, 93
- Installationsfehler, 133
- Installierte Pakete, 16
- Java Messaging Service, 111–112, 114
- java.lang.OutOfMemoryError: PermGen-Speicher, 133
- jBoss, 109
- JBoss-Messaging, 111
- JBoss-Naming-Factory, 111
- JD Edwards (JDE), 48, 54
- JDBC, 135
- JDBC-Treiber, 135
- JDE-Anwendungsbenutzer (Sicherheits-Provider), 48, 54
- JMS, 111–112, 114
- JMS-Bus, 139
- JMS-Client-Beispielprogramm, 112
- JMS-Meldungsdomäne, 112, 114
- JMS-Thema-Konfiguration, 111
- JMS-Themen, 111
- JMS-Warteschlange, 111
- JNDI, 111–112
- jndi.properties, 112
- Job-Ausführungsereignisse, 117
- Job-Ausgabe
 - Anzeigen, 105
- Jobschritt-Verlauf, 103
- Jobstatus, 103
- Kerberos
 - Domäne, 60
 - JAAS, 60
 - Key Distribution Center (Schlüsselverteilungszentrale), 60
 - Realm, 60
 - Schlüsseltabellendatei, 60
 - Service-Ticket, 60
- Komponenten, 16
- Konfiguration , 62–64, 66–68, 70, 76–77, 79, 82–87
 - Bewertung, 68
 - Deployment Portal-Scoring, 68
 - Optionen, 105
- Konfigurieren
 - ATOM, 70
 - Benachrichtigung, 70
 - Benutzerdefinierte Dialogfelder, 65
 - Cache, 64
 - Datenservice, 66
 - Deployment Manager, 67
 - Deployment Portal, 67
 - Enterprise-Ansicht, 68
 - Hilfe, 62, 70
 - IBM ShowCase Warehouse Builder, 86
 - IBM SPSS Statistics, 65
 - pager, 76
 - Prozessmanagement, 77
 - Repository, 79
 - RSS, 70
 - Setup, 85
 - Sicherheit, 62, 84
 - Syndication, 70
 - System, 62–64, 66–68, 70, 76–77, 82–87
 - URL-Präfix, 85
 - Vorlagen, 62–63
- Konsole
 - UNIX, 9, 12
 - Windows, 9, 12
- Konventionen
 - Benennen, 23
- Kürzungsfehler
 - Korrektur, 87
- LD_LIBRARY_PATH, 135
- LDAP, 48
- legal notices, 145

- Leistungsengpässe, 133
- LIBPATH, 135
- Lokale Gruppen
 - für Active Directory, 57
- lokale Überschreibung
 - für Active Directory, 48
- Lokaler Principal-Filter
 - für Active Directory, 57
- Lokaler Sicherheits-Provider, 25–26
- Lokales Benutzer-Repository, 48
- löschen
 - Benutzer, 33
 - groups, 36
 - MIME-Typen, 92
 - Verwaltete Server, 23

- Meldungsbasierte Zeitplanung, 111–112, 114
- messageContent-Element
 - contentType-Attribut, 100
 - in Benachrichtigungsvorlagen, 95, 98, 100
- messageProperty-Element
 - in Benachrichtigungsvorlagen, 95–96
- messageSubject-Element
 - in Benachrichtigungsvorlagen, 95, 98
- MIME, 89
- MIME-Typen, 89, 100
 - bearbeiten, 91
 - hinzufügen, 90
 - löschen, 92
- mimeMessage-Element
 - in Benachrichtigungsvorlagen, 95

- Namenskonventionen, 23
- Nationale Zeichensätze, 136
- Nativer Provider, 48, 50, 52, 54, 56–57
- nativestore-Element, 141
- Nativestore-Schema, 141
- Navigation, 9, 15
- Neuindizierung, 93
- Neuinstallation des Repository, 135
- NFS, 136
- nslookup, 110

- obsolete-Element
 - in nativestore, 141, 143
- OpenJMS, 111
- OpenLDAP, 25–26, 58
 - Aktivieren, 51
 - Deaktivieren, 51
- Oracle
 - Fehler, 137
- Oracle AQ, 111
- Ordner
 - Benennen, 23

- password-Attribut
 - für user, 142
- Passwörter, 135
 - ändern, 9, 14
 - Angeben, 13
 - Bereitstellen, 13
- Patches, 140
- PDF, 136
- PEB-Bericht Verarbeitungsfehler, 135
- Permanente Generation Heap-Größe, 134
- Persistente Ereigniswarteschlange, 105
- Portnummern, 21
- Protokoll-Zeitbeschränkung, 67
- Protokolle, 16
- Provider, 48
- Prozessmanagement
 - Konfiguration, 77

- Registerkarten
 - Navigieren, 15
- Remote-Verarbeitung
 - Ausführungsserver, 6
- Repository
 - Konfiguration, 79
- Repository-Ereignisse, 117
- RFC3461, 109
- Richtlinien
 - Benennen, 23
- role-Element
 - in user, 141, 143
- Rollen, 25–26, 40
 - Administratoren, 42
 - bearbeiten, 45
 - entfernen, 47
 - Entfernen von Aktionen, 45
 - erstellen, 43
 - hinzufügen, 45
 - Hinzufügen von Aktionen, 45
 - Zuweisen von Benutzern, 45
 - Zuweisen von Gruppen., 45
- RSS-Feeds, 70

- SAS
 - Ausführungsserver, 6
- Schema
 - Auditing der Datenbank, 118
- Schlüsselspeicher-Datei, 135
- Schriftarten, 136
- Scoring-Konfigurationen, 68
- Scoring-Service, 82, 136
- Seiten
 - Anmelden, 13–14, 62
 - Benachrichtigung, 70
 - Datenservice, 66
 - Deployment Portal, 67
 - IBM ShowCase Warehouse Builder, 86
 - Konfiguration, 62–63, 66–68, 70, 77, 79, 83–87

- pager , 76

- Prozessmanagement, 77
- Repository, 79
- SMTP-Einstellungen, 70
- Suchen, 83
- Server
 - starten, 9
 - Stoppen, 9, 12
 - UNIX, 9, 12
 - Windows, 9, 12
- Services
 - UNIX, 9, 12
 - Windows, 9, 12
- Setup, 135
 - Konfiguration, 85
- SHLIB_PATH, 135
- Sicherheit, 62, 84
- Sicherheits-Provider, 25–26, 48–49
 - Active Directory, 50, 56
 - Active Directory mit lokaler Überschreibung, 51, 57
 - Aktivieren, 56
 - Deaktivieren, 56
 - IBM i, 52
 - IBM i nativ, 57
 - IBM i-Benutzer-Repository, 48
 - JDE-Anwendungsbenutzer, 54
 - nativ, 50, 56
 - OpenLDAP, 51, 58
 - SiteMinder, 54, 58
- Sicherheitsereignisse, 117
- Sicherungskopie der Schlüsselspeicher-Datei, 135
- SiteMinder, 49, 54, 58
- siteminder.package, 49
- Sitzungs-Zeitüberschreitung, 84
- SMTP
 - Eigenschaften, 96
 - Meldungsvorspann, 110
 - Protokollierung, 109
 - Server-Threads, 105
- Solaris 10, 136
- Solaris 9
 - Fehler, 136
 - libm.so.1, 136
 - libm.so.2, 136
 - Startfehler, 136
 - Wrapper-Fehler, 136
- Speicherfehler, 133–134
- Speichermangel-Fehler, 134
- Speicherzuteilung, 134
- SQL-Abfragen, 116
- SSL, 21, 50, 57
- SSO, 13, 48, 57
- Suchdienst, 93
- Suchen, 83
- Suchlimit, 84
- Sun Java System Message Queue, 111
- SVG-Diagramme, 63
- Symbolische Verknüpfung, 136
- System
 - Abmeldung, 9
 - Anmelden, 9, 13–14
 - Konfigurieren, 62–68, 70, 77, 79, 82–87
 - Navigation, 9, 15
 - starten, 9, 13–15
 - Starten, 9, 12–14
 - Stoppen, 12
 - Übersicht, 14, 23
- Systemfehler, 133, 136–137
- Systeminformationen, 16
- Tablespaces, 137
- Thema, 111
- Themen
 - Benennen, 23
- trademarks, 146
- Treiber-URL, 135
- Übersicht, 13–14, 23
- Umgebungsvariablen, 135
- UNIX
 - Services, 9, 12
- URL-Präfix, 85
- user-Element
 - in nativestore, 141–142
 - in obsolete, 143
- userID-Attribut
 - für user, 142
- value-of-Element
 - in Benachrichtigungsvorlagen, 96, 98
- Velocity, 95
- Verschlüsselung, 135
- Version, 16
- Verwaltete Server
 - Abmelden, 22
 - Anmeldung, 22
 - Eigenschaften, 21
 - hinzufügen, 18
 - löschen, 23
 - Serverinformationen, 20
 - Typen, 18
- Verzeichnispfad, 79
- Visualisierung
 - Berichte, 79
 - Spezifikationen, 79
- Vorlagen, 62–63
 - Anpassen von Eigenschaften, 96
 - Anpassen von Format, 100
 - Anpassen von Inhalten, 98
 - Eigenschaften einfügen, 98
 - Einfügen von Ereigniseigenschaftsvariablen, 98
 - für E-Mail-Benachrichtigungen, 95, 102
 - Velocity, 102

Index

Warteschlange, 111
WebSphere, 139
WebSphere MQ, 111
Wiederherstellen, 140
Windows
 Services, 9, 12
Wrapper-Fehler, 136
Wrapper-Service, 133

Zeichenbeschränkung
 für benutzerdefinierte Funktionen, 87
Zeichenbeschränkung für UDF, 87
Zeitbeschränkungsfehler, 67
Zusammenarbeit, 1
Zustellungsfehler, 110