IBM SPSS Collaboration and Deployment Services 5 Administratorhandbuch

Hinweis: Lesen Sie vor der Verwendung dieser Informationen und des zugehörigen Produkts die allgemeinen Informationen unter Hinweise auf S. 144.

Diese Ausgabe gilt für IBM SPSS Collaboration and Deployment Services 5 und alle nachfolgenden Versionen und Abwandlungen, bis in neuen Ausgaben anderweitig angegeben.

Screenshots von Adobe-Produkten nachgedruckt mit Genehmigung durch Adobe Systems Incorporated.

Screenshots von Microsoft-Produkten nachgedruckt mit Genehmigung durch Microsoft Corporation.

Lizenziertes Material – Eigentum von IBM

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 5-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 5-Benutzerhandbuch* beschrieben.

Technischer Support

Registrierte Kunden von IBM Corp. können den IBM Corp. Technischen Support in Anspruch nehmen. Kunden können sich an den technischen Support wenden, wenn sie Hilfe bei der Arbeit mit IBM Corp.-Produkten oder bei der Installation in einer der unterstützten Hardware-Umgebungen benötigen. Informationen zum Technischen Support finden Sie auf der IBM Corp.-Website unter *http://www.spss.com* oder wenden Sie sich an Ihr regionales Büro, das Sie auf der IBM Corp.-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 IBM Corp.-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.

Inhalt

Kapitel
1

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 Sicherungs- 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. 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 Repositorys 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 einzelne, im Repository gespeicherte Dateien in Verarbeitungs-**Jobs** aufgenommen werden. Jobs legen eine Ausführungsreihenfolge für analytische Artefakte fest und können mit IBM® SPSS® Collaboration and Deployment Services Deployment Manager erstellt werden. Die Ausführungsergebnisse können im Repository oder auf einem Dateisystem gespeichert oder an angebebene 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.

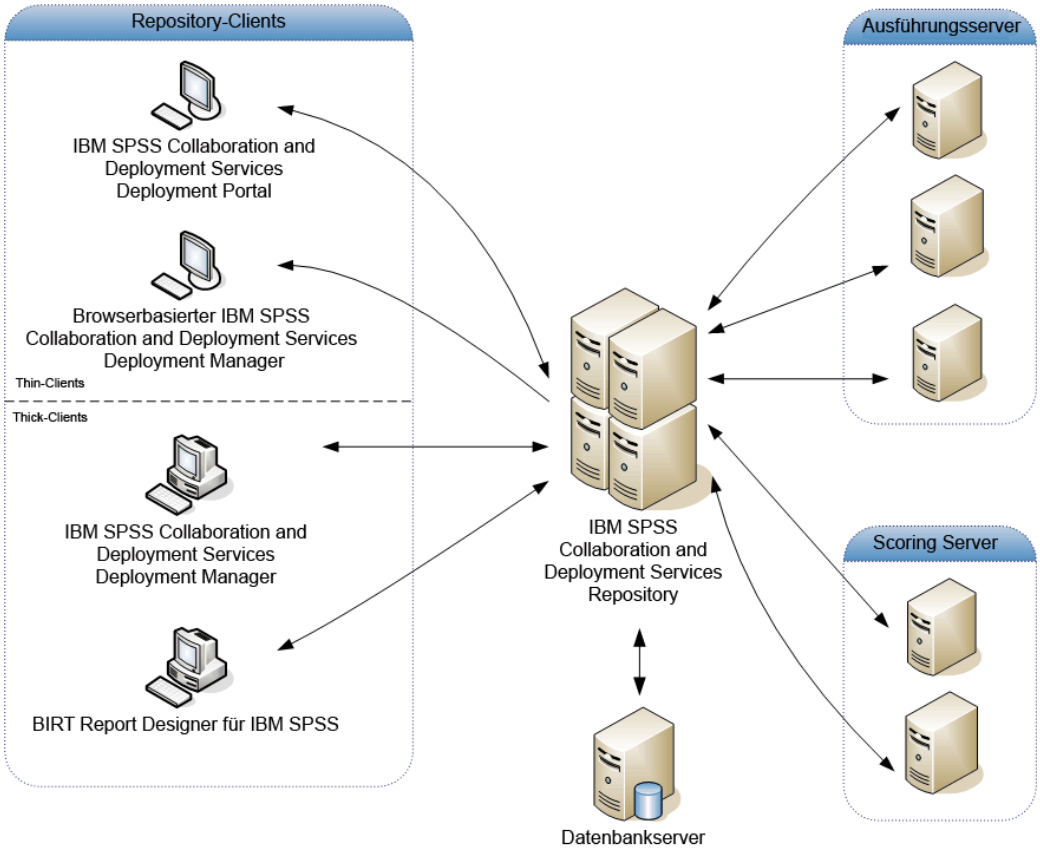
Zusätzlich gestattet der Scoring-Service von IBM SPSS Collaboration and Deployment Services, dass Analyseergebnisse von bereitgestellten Modellen bei der Interaktion mit einem Kunden in Echtzeit geliefert werden. Ein für Scoring konfiguriertes Analysemodell kann Daten, die in einer aktuellen Kundeninteraktion 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
- 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
- Versionskontrolle

- Suchen
- Auditing

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

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 Repositorys 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 für IBM® SPSS® Collaboration and Deployment Services Repository, die es Benutzern ermöglicht, Analyseaufgaben, wie die Aktualisierung von Modellen oder das Generieren von Scores, 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:

- Benutzer verwalten
- Sicherheits-Provider konfigurieren
- Rollen und Aktionen zuweisen

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:

- Festlegen von Optionen zur Systemkonfiguration
- 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 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 Benutzervoreinstellungen wie E-Mail-Adresse und Passwort, auf allgemeine Optionen, Abonnements und Optionen für Ausgabedateiformate

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 JDBC- und ODBC-Treiber, mit der Ausnahme, dass er nicht direkt eine physische Datenquelle abfragt, sondern vielmehr die physischen Datenquellen entsprechend dem

Design der Daten-Provider-Definitionen virtualisiert. Beachten Sie, dass Enterprise-Ansicht als Teil von IBM® SPSS® Collaboration and Deployment Services Deployment Manager installiert wird, der IBM SPSS Collaboration and Deployment Services Enterprise View Driver-Treiber jedoch separat installiert werden muss. Weitere Informationen finden Sie in der IBM SPSS Collaboration and Deployment Services Enterprise View Driver-Dokumentation.

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.

Scoring Server

IBM® SPSS® Collaboration and Deployment Services Scoring Service ist auch als separat bereitstellbare Anwendung, als so genannter Scoring Server, verfügbar. Der Scoring Server verbessert die Bereitstellungsflexibilität in mehreren wichtigen Bereichen:

- Die Scoring-Leistung kann unabhängig von anderen Diensten skaliert werden.
- Scoring Server können unabhängig voneinander konfiguriert werden, um Computerressourcen einer oder mehreren IBM SPSS Collaboration and Deployment Services-Scoring-Konfigurationen zuzuteilen.
- Betriebssystem und Prozessorarchitektur des Scoring Servers brauchen nicht mit dem IBM® SPSS® Collaboration and Deployment Services Repository oder anderen Scoring Server-Instanzen übereinzustimmen.
- Der Scoring Server-Anwendungsserver braucht nicht mit dem Anwendungsserver übereinzustimmen, der für IBM SPSS Collaboration and Deployment Services Repository oder andere Scoring Server verwendet wird.

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*).

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.

IBM SPSS Decision Management

IBM® SPSS® Collaboration and Deployment Services sind eine Voraussetzung für die Installation von IBM® SPSS® Decision Management, einer Anwendungssuite zur Integration von Vorhersageanalysen in die betrieblichen Entscheidungsfindungsprozesse. SPSS Decision Management verwendet schnelles Scoring, Masterdaten-Management und Funktionen zur Prozessautomatisierung von IBM SPSS Collaboration and Deployment Services zur Optimierung und Automatisierung von Entscheidungen mit hohem Volumen sowie zum Erstellen verbesserter Ergebnisse in bestimmten Geschäftssituationen.

IBM ShowCase

IBM® SPSS® Collaboration and Deployment Services kann unter IBM i bereitgestellt werden, um die Integration mit der IBM® ShowCase® Business-Intelligence-Suite zu ermöglichen und so eine Berichterstellungsplattform auf Unternehmensebene bereitzustellen, mit der Informationen effizient, sicher und kosteneffektiv an eine beliebige Anzahl an Personen verteilt werden können. Mit dieser Berichterstellungsumgebung können Sie ein zentralisiertes, sicheres und durchsuchbares Repository für IBM® ShowCase® Query- und IBM® ShowCase® Report Writer-Inhalte erstellen, Benutzern einen einfachen Zugang zu Inhalten und Berichtsausgaben über eine Webbrowser-basierte Oberfläche ermöglichen, Abfrage- und Berichtsdefinitionen für geplante und dynamische Ausführung über das Web freigeben, Excel-Tabellen veröffentlichen,

die für die Aktualisierung geplant oder dynamisch über einen Webbrowser aktualisiert werden können, und Berichte erstellen, die Diagramme, Bilder und Links auf andere Berichte enthalten.

Wichtig: Die Funktionen für schnelles Scoring von IBM SPSS Collaboration and Deployment Services stehen unter IBM i nicht zur Verfügung.

Kapitel
2

Neuerungen in dieser Version

Neuerungen für Administratoren

IBM® SPSS® Collaboration and Deployment Services 5 bietet neue Funktionen, die die Bereitstellung von Vorhersageanalysen erleichtern und die Ihnen helfen, die Kosten besser in den Griff zu bekommen.

Sicherheits-Provider-Definition

Sicherheits-Provider werden nun über eine Assistenten-Oberfläche definiert, die eine größere Kontrolle über die Provider-Einstellungen gestattet. Für weitere Informationen siehe Thema Konfigurieren von Sicherheits-Providern in Kapitel 7 auf S. 52.

Kontosperrung

Laut Standardeinstellung wird das Benutzerkonto eines nativen Benutzers des lokalen Benutzer-Repositorys, der dreimal in Folge versucht, sich mit einem falschen Kennwort bei IBM SPSS Collaboration and Deployment Services anzumelden, automatisch gesperrt. Der Benutzer kann sich nicht mehr anmelden (auch nicht mit den richtigen Anmeldedaten), bis die Sperre für sein Konto nach dreißig Minuten automatisch oder manuell durch einen Administrator aufgehoben wurde. Für weitere Informationen siehe Thema Sperren und Entsperren von Benutzern in Kapitel 4 auf S. 32.

Cross-Site Scripting-Filter

Cross Site Scripting (XSS) ist eine Computer-Sicherheitslücke, die häufig in Webanwendungen zu finden ist. Sie ermöglicht Angreifern, die clientseitigen Sicherheitsmechanismen zu umgehen, die normalerweise von modernen Webbrowsern für Webinhalte implementiert werden, indem sie ein schädliches Skript in von anderen Personen angezeigte Webseiten einbringt. In früheren Versionen von IBM SPSS Collaboration and Deployment Services stand ein Web-Sicherheitsfilter zur Verfügung, um XSS-Attacken durch die Überprüfung der vom Benutzer eingegebenen Parameter zu verhindern. Die Filterkriterien konnten jedoch nicht geändert werden. Nun können Sie XSS-Filterregeln entsprechend der für Ihr Unternehmen geltenden Sicherheitsrichtlinie hinzufügen, ändern und löschen.Für weitere Informationen siehe Thema XSS-Filter (Cross Site Scripting) in Kapitel 6 auf S. 49.

Dokumentation

Der Zugriff auf die vollständige IBM SPSS Collaboration and Deployment Services-Dokumentation ist nun im Internet über ein IBM Information Center möglich: *http://publib.boulder.ibm.com/infocenter/spsscads/v5r0m0/index.jsp*. Die Dokumentation wurde um folgende Handbücher erweitert:

- Handbuch zur Fehlerbehebung
- Quickstart-Handbuch

Kapitel
3

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 des 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 wird durch Starten des Anwendungsservers gestartet. Dies kann mit den Skripts durchgeführt werden, die mit der Repository-Installation bereitgestellt werden, oder mit den nativen Administrations-Tools des Anwendungsservers. Weitere Informationen finden Sie in der Herstellerdokumentation zum Anwendungsserver.

WebSphere

Verwenden Sie WebSphere-Administrationstools. Weitere Informationen finden Sie in der WebSphere-Dokumentation.

JBoss

Verwenden Sie folgende Skripts für die Repository-Installation:

<Repository-Installationsverzeichnis>/bin/startserver.cmd

<Repository-Installationsverzeichnis>/bin/startserver.sh

Alternativ können Sie auch JBoss-Administrationstools zum Starten des Servers verwenden. Weitere Informationen finden Sie in der JBoss-Dokumentation.

WebLogic

Verwenden Sie bei Konfigurationen mit einem einzelnen WebLogic-Server die folgenden, bei der Repository-Installation bereitgestellten Skripts:

<Repository-Installationsverzeichnis>/bin/startserver.cmd

<Repository-Installationsverzeichnis>/bin/startserver.sh

Der WebLogic-Anwendungsserver kann auch mit Ihrer bevorzugten Methode gestartet werden, Sie müssen jedoch sicherstellen, dass die richtigen Umgebungsvariablen und Java-Eigenschaften festgelegt werden. Zur Unterstützung dieses Vorgangs erstellt der Konfigurationsvorgang folgende Skripts im Verzeichnis *toDeploy/current*:

- *setCDSEnv.cmd* bzw. *setCDSEnv.sh*
- *startCDSWebLogic.cmd* bzw. *startCDSWebLogic.sh*
- *startManagedCDSWebLogic.cmd* bzw. *startManagedCDSWebLogic.sh*

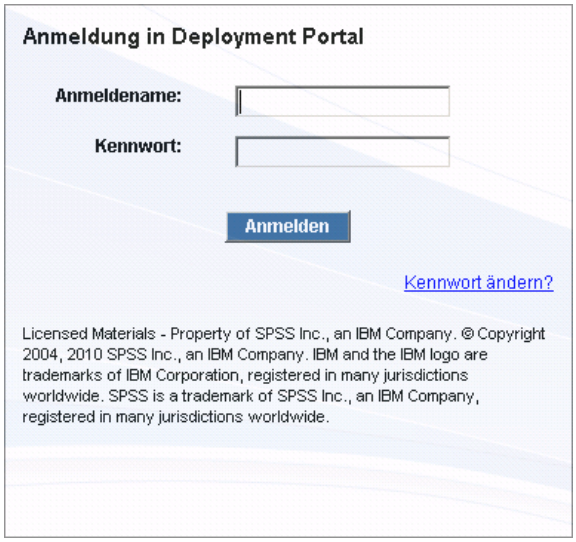
Wenn Sie während der Konfiguration die automatische Bereitstellung ausgewählt haben, werden die Dateien auch in die Domäne und in das Verzeichnis *<Domäne>/bin* kopiert. Untersuchen Sie diese Dateien, um zu ermitteln, welche Umgebungs- und Java-Eigenschaften festgelegt werden müssen. Die konkreten Eigenschaften variieren je nach den installierten IBM SPSS-Adaptern. Wenn Sie Ihren Server mit einem Startskript starten, können Sie *setCDSEnv.cmd/setCDSEnv.sh* über dieses Skript aufrufen. Wenn Sie den Knotenmanager oder eine andere Methode zum Starten des Servers verwenden, müssen Sie darauf achten, die entsprechenden Einstellungen zu definieren.

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. Typischerweise lautet der URL 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"



- Geben Sie in das Feld "Anmeldenamen" 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. 13.

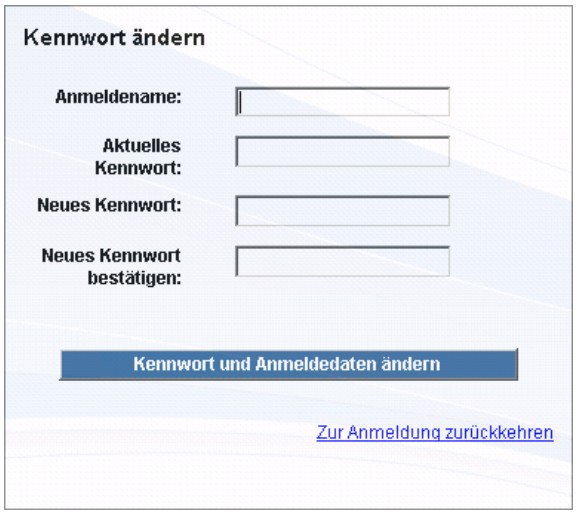
Wichtig: Einzelanmeldung ist für browserbasiertes IBM® SPSS® Collaboration and Deployment Services Deployment Manager nicht gestattet.

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



- 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. 12.

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.

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

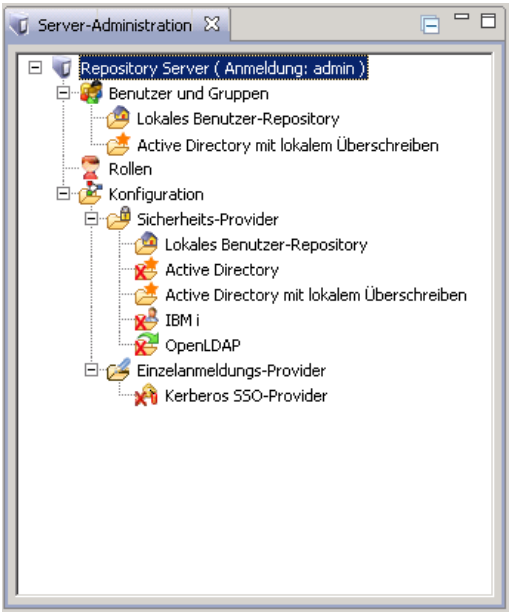
Die Server-Administration in IBM® SPSS® Collaboration and Deployment Services Deployment Manager umfasst:

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.

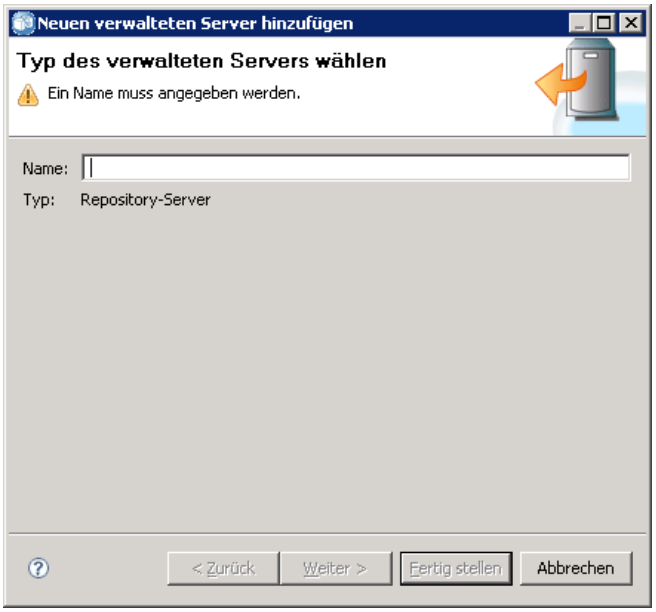
Wählen Sie die folgenden Befehle aus den Menüs aus:
Datei > Neu > Verwaltete Server-Verbindung

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" identifziert wird. Die Angabe der Portnummer, z. B. *my_server:8080*, kann helfen, den Server in der Liste der verwalteten Server zu identifzieren.

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.

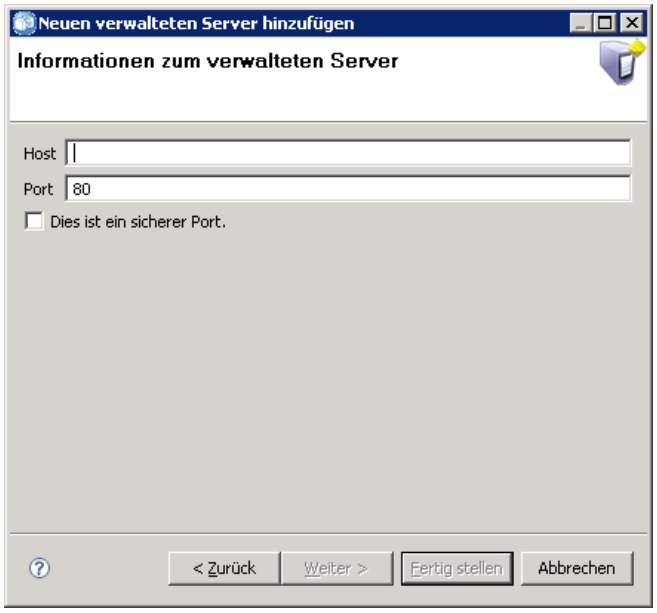
2. Wählen Sie den Servertyp aus.

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:

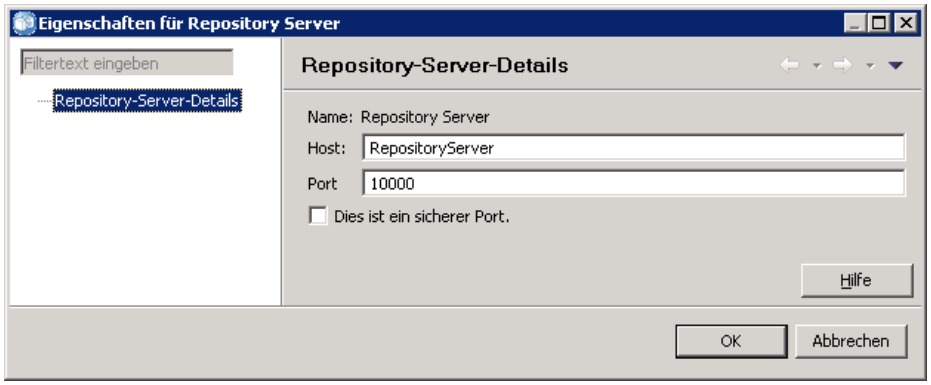
1. Geben Sie den Hostnamen oder die IP-Adresse des Servers ein, der hinzugefügt wird.
2. Geben Sie die Portnummer an, an der der hinzugefügte Server ausgeführt werden soll.
3. Geben Sie an, ob der Server SSL verwendet, falls zutreffend.
4. Klicken Sie auf Fertig stellen.

   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



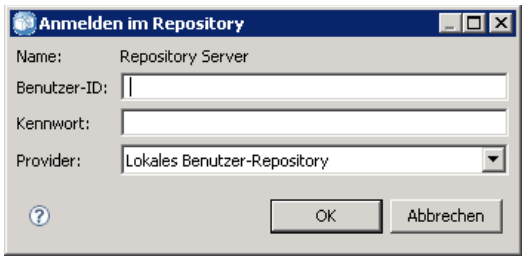
Eigenschaften für Repository-Server:

- **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.

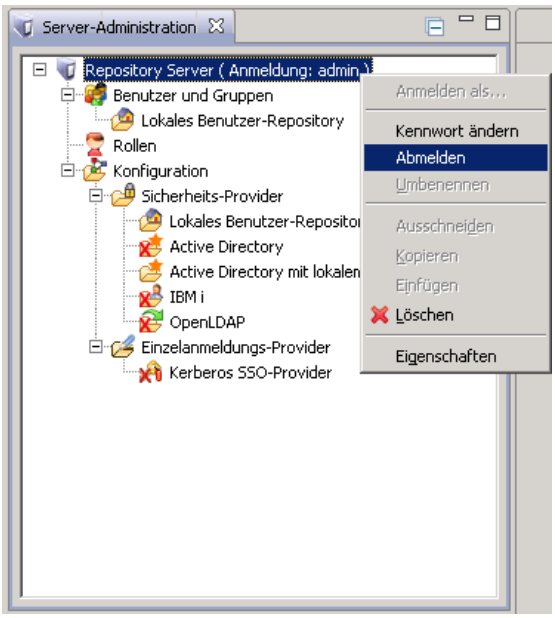
Anbieter. Der Provider, für den die angegebene Anmeldung-Passwort-Kombination geprüft werden muss. Dieses Feld wird nur angezeigt, wenn mehrere Sicherheits-Provider für das System aktiviert sind. Andernfalls validiert das System die angegebenen Anmeldedaten im lokalen Benutzer-Repository.

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.

Kapitel
4

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. 41.

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 7 auf S. 51.

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. 46. 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. 44.

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 7 auf S. 52.
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.

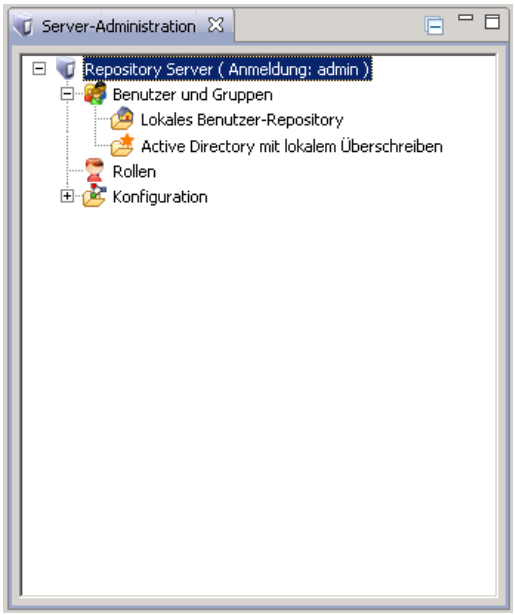
Verwalten von Benutzern und Gruppen in IBM SPSS Collaboration and Deployment Services Deployment Manager

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”

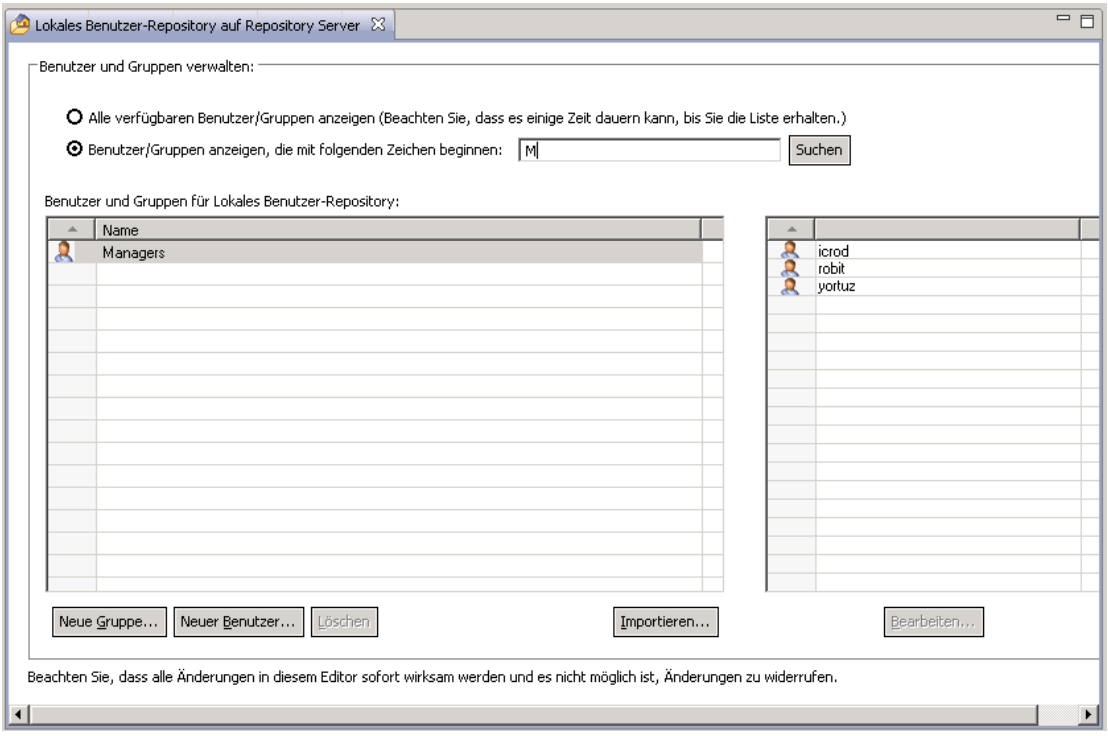


3. Doppelklicken Sie auf das Symbol Lokales Benutzer-Repository oder Active Directory mit lokalem Überschreiben.

   Der Editor “Benutzer und Gruppen verwalten” wird geöffnet.

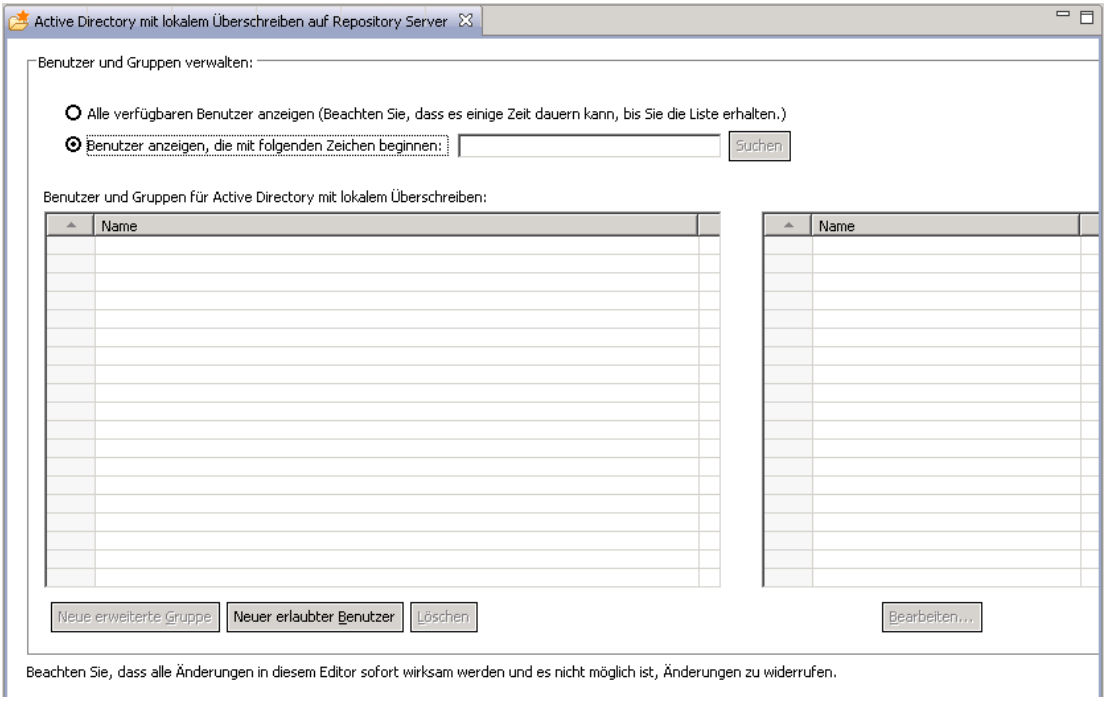
   - Für “Lokales Benutzer-Repository” zeigt der Editor alle nativen Benutzer und Gruppen oder eine gefilterte Liste auf der Basis der Anfangsbuchstaben in den Benutzer- und Gruppennamen. Ein Administrator kann Benutzer und Gruppen erstellen und löschen, die Eigenschaften von bestehenden Benutzern und Gruppen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

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 7 auf S. 51.

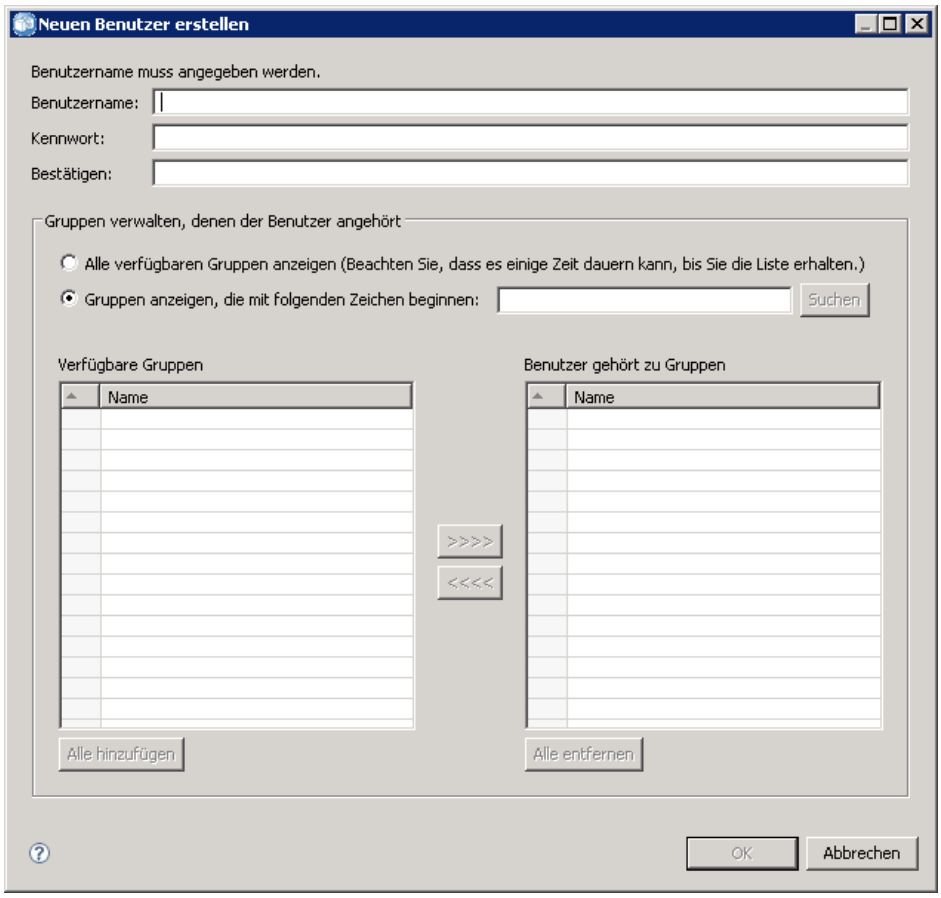
Abbildung 4-3
Editor "Benutzer und Gruppen verwalten" für Active Directory mit lokalem Überschreiben



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.

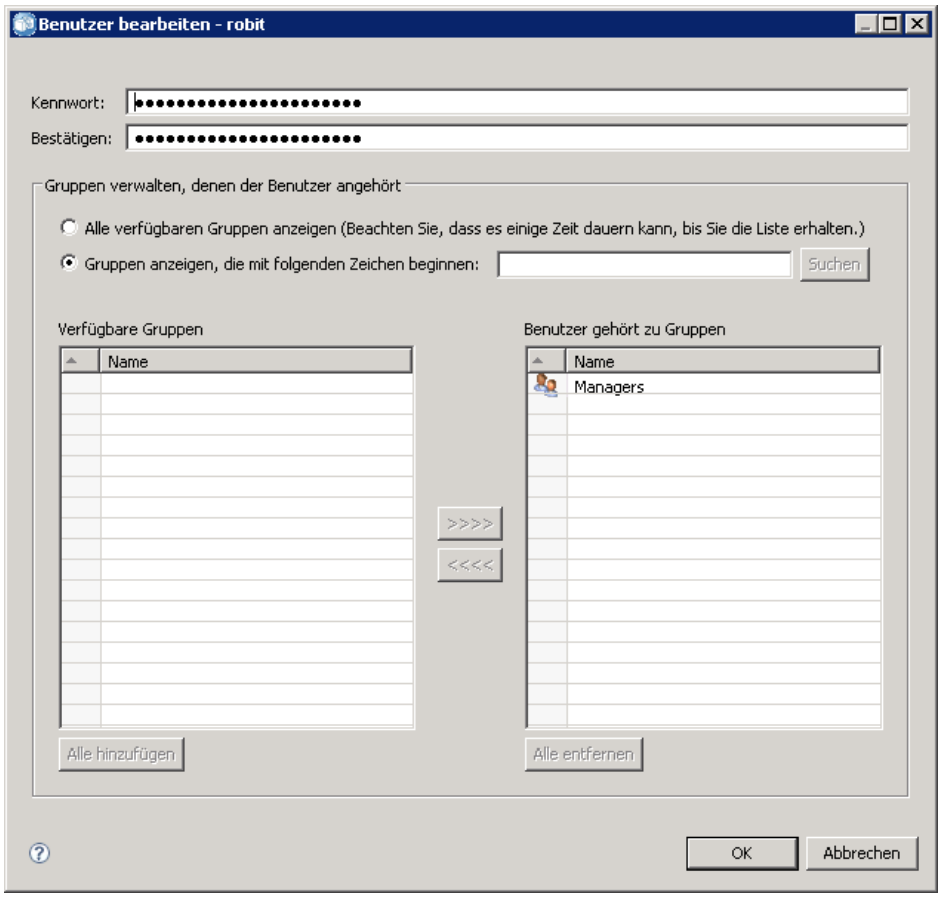
Für das Erstellen eines lokalen Benutzers müssen Anmeldedaten angegeben werden. Der Benutzer kann außerdem mit Gruppen assoziiert werden.

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.

Sperren und Entsperren von Benutzern

Laut Standardeinsteller wird das Benutzerkonto eines nativen Benutzers des lokalen Benutzer-Repositorys, der dreimal in Folge versucht, sich mit einem falschen Kennwort bei IBM® SPSS® Collaboration and Deployment Services anzumelden, automatisch gesperrt. Der Benutzer kann sich nicht mehr anmelden (auch nicht mit den richtigen Anmeldedaten), bis die Sperre für sein Konto nach dreißig Minuten automatisch oder manuell durch einen Administrator aufgehoben wurde.

Im browserbasierten IBM® SPSS® Collaboration and Deployment Services Deployment Manager, im Abschnitt “Sicherheit”, gibt es zwei Konfigurationseinstellungen zur Anpassung dieser Funktion:

- **Zählerschwellenwert für ungültige Anmeldeversuche.** Mit dieser Einstellung wird festgelegt, wie oft eine fehlgeschlagene Anmeldung zulässig ist, bevor der Benutzer automatisch gesperrt wird. Sie können auch festlegen, dass die Benutzer nie automatisch gesperrt werden sollen.
- **Dauer der Kontosperre.** Mit dieser Einstellung wird die Wartezeit in Minuten festgelegt, bis die Sperre für gesperrte Benutzer aufgehoben wird. Sie können auch festlegen, dass die Sperre von Benutzern nie automatisch aufgehoben werden soll.

Beachten Sie, dass sich diese Funktion ausschließlich auf die Benutzer des Native-Sicherheits-Providers “Lokales Benutzer-Repository” bezieht.

Im Editor “Benutzer und Gruppen verwalten” für “Lokales Benutzer-Repository” haben Sie außerdem die Möglichkeit, lokale Benutzer manuell zu sperren bzw. die Sperre aufzuheben. Die Spalte “Status” gibt an, ob ein Benutzer gesperrt ist. Um alle Benutzer anzuzeigen, die derzeit gesperrt sind, wählen Sie im Editor “Benutzer und Gruppen verwalten” die Option Nur gesperrte Benutzer anzeigen aus.

So heben Sie die Sperre eines lokalen Benutzers manuell auf:

1. Wählen Sie den gesperrten Benutzer im Editor “Benutzer und Gruppen verwalten” aus. In der Spalte “Status” wird für alle gesperrten Benutzer der Text Gesperrt angezeigt. Wenn Sie alle derzeit gesperrten Benutzer anzeigen möchten, klicken Sie auf Nur gesperrte Benutzer anzeigen.
2. Klicken Sie auf Entsperren. Ein Dialogfeld wird geöffnet, in dem Sie bestätigen können, dass die Sperre des Benutzers aufgehoben werden soll.
3. Klicken Sie auf Ja, um die Sperre des Benutzers aufzuheben.

So sperren Sie einen lokalen Benutzer manuell:

1. Wählen Sie den zu sperrenden Benutzer im Editor “Benutzer und Gruppen verwalten” aus. Gruppen können nicht gesperrt werden.
2. Klicken Sie auf Sperren. Ein Dialogfeld wird geöffnet, in dem Sie bestätigen können, dass der Benutzer gesperrt werden soll.
3. Klicken Sie auf Ja, um den Benutzer zu sperren. Beachten Sie, dass manuell gesperrte Benutzer gesperrt bleiben, bis die Sperre manuell wieder aufgehoben wird. Die weiter oben beschriebene

Konfigurationseinstellung “Dauer der Kontosperre” findet keine Anwendung (die Sperre des Benutzers wird nicht automatisch aufgehoben).

Löschen eines Benutzers

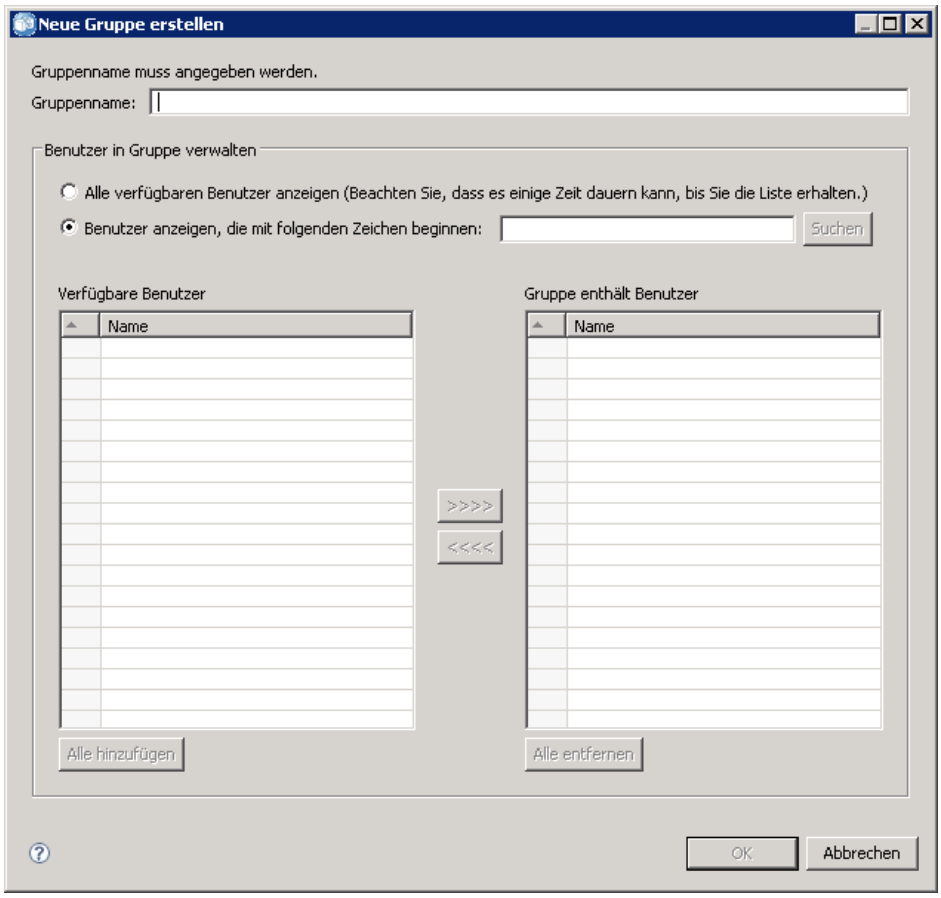
So löschen Sie einen lokalen Benutzer oder einen erlaubten Benutzer in Active Directory mit lokalem Überschreiben:

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.

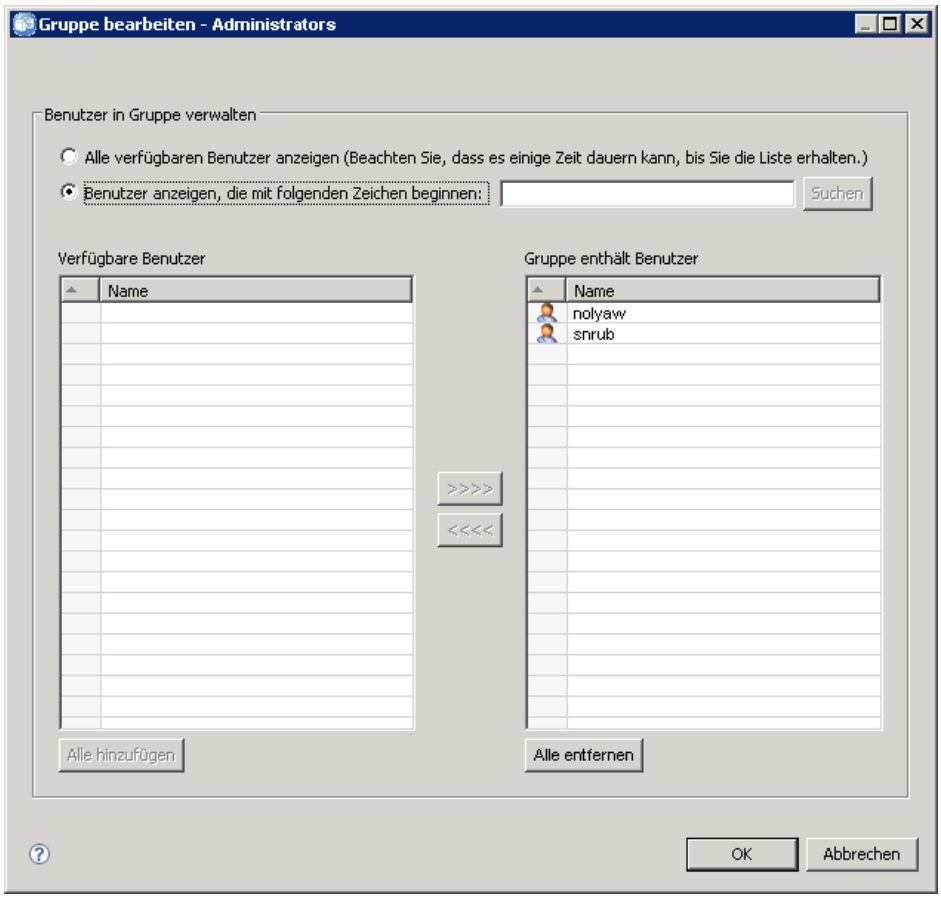
Für das Erstellen einer lokalen Gruppe muss der Benutzername angegeben werden. Der Gruppe können auch Benutzer hinzugefügt werden.

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.

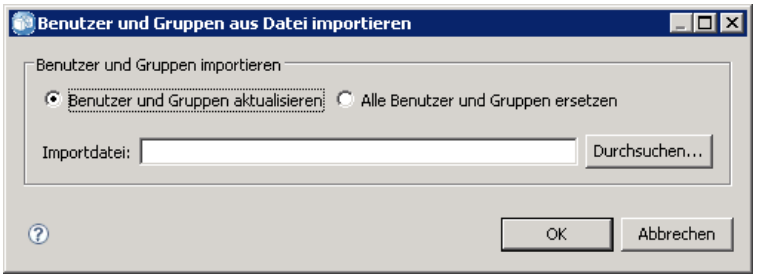
Importieren von Benutzern und Gruppen

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 A.

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.

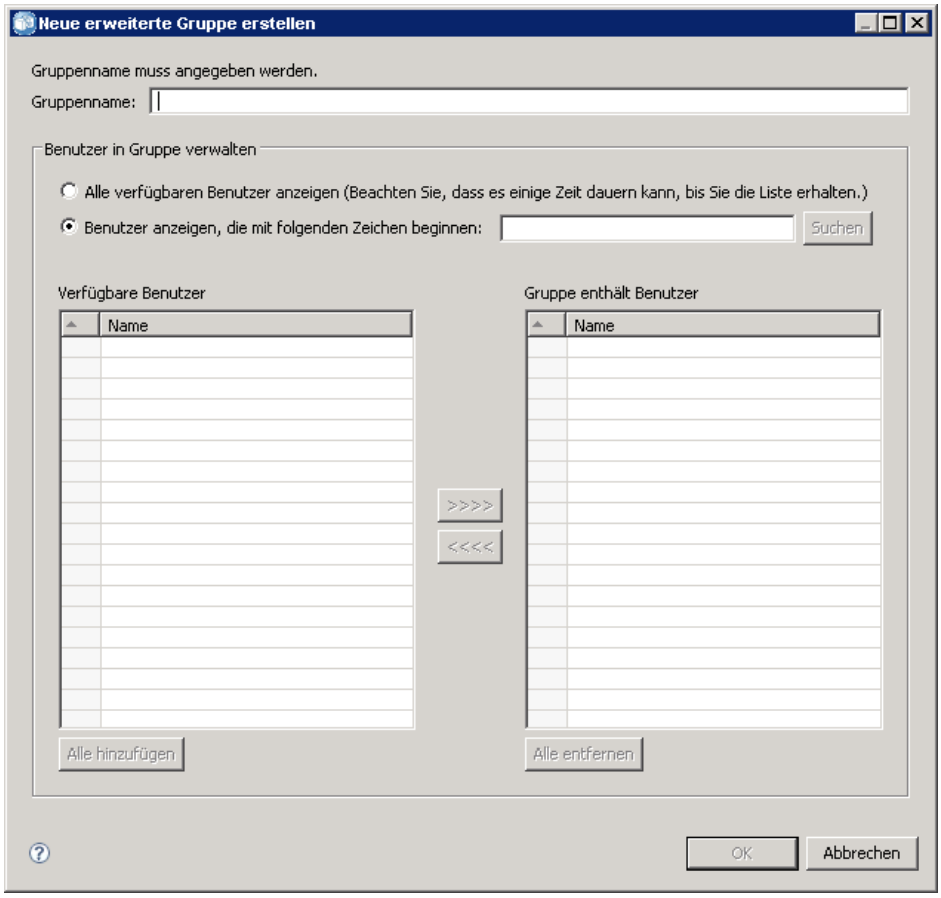
3. Navigieren Sie zum Speicherort der Importdatei.

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.

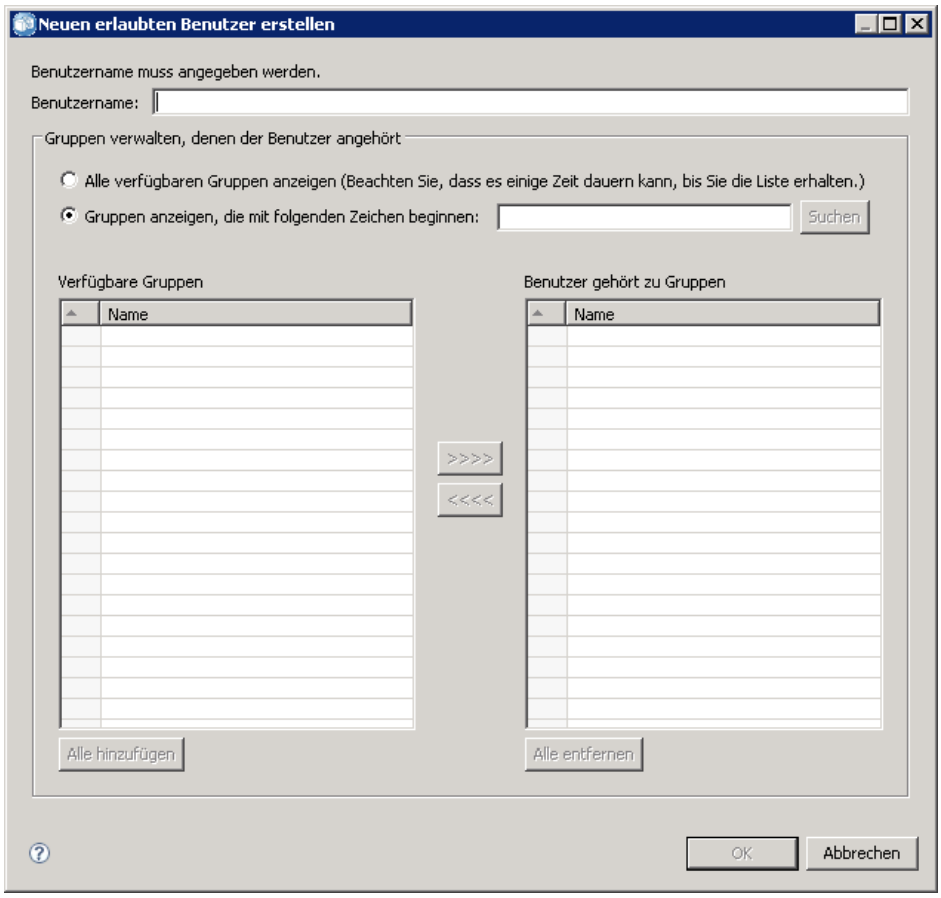
Für das Erstellen einer erweiterten Gruppe muss der Benutzername angegeben werden. Der Gruppe können auch Benutzer hinzugefügt werden.

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”.

Kapitel
5

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 Repositorys 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 dagegen 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 Repositorys.
- **Datenquellen definieren.** Definieren und Bearbeiten von Datenquellen.
- **Meldungsdomänen definieren.** Definieren und Bearbeiten von Domänen für JMS-Meldungen.
- **Höherstufungsrichtlinien definieren.** Definieren und Bearbeiten von Richtlinien (Regelsätzen) zur Höherstufung von Repository-Objekten.
- **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.
- **Objekte höherstufen.** Höherstufen von Repository-Objekten.
- **Repository-Index.** Erstellen eines neuen Index für den Inhalt des Repositorys.
- **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. Beachten Sie, dass IBM SPSS Collaboration and Deployment Services-Produkte keine Benutzerschnittstellen zur Bearbeitung der Voreinstellungen anderer Benutzer aufweisen. Diese Einstellung gilt nur, wenn der User Preference Web Service (Webdienst für Benutzervoreinstellungen) direkt aufgerufen wird.
- **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

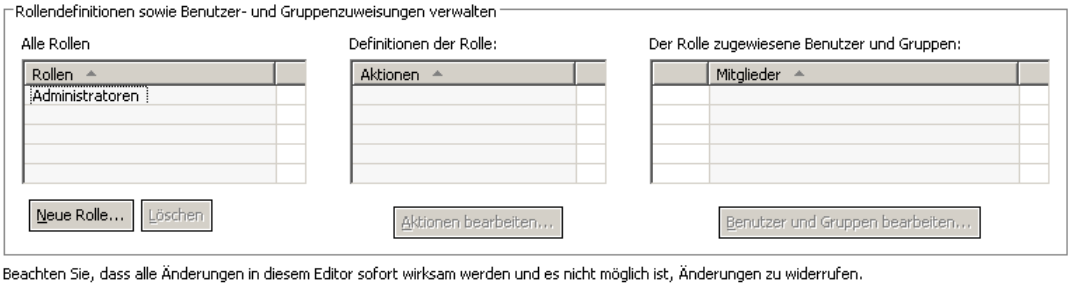
Das System umfasst eine vordefinierte Rolle für *Administratoren*, die nicht geändert werden kann. Diese Rolle ist mit allen im System verfügbaren Aktionen verknüpft. Jeder Benutzer mit dieser Rolle kann jede beliebige Aktion im System ausführen. Zudem steht einige Funktionalität, die nicht durch Aktionen 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. 44.

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 Rolllen, damit der Server auf den Editor “Rollendefinitionen verwalten” zugreift.

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



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.

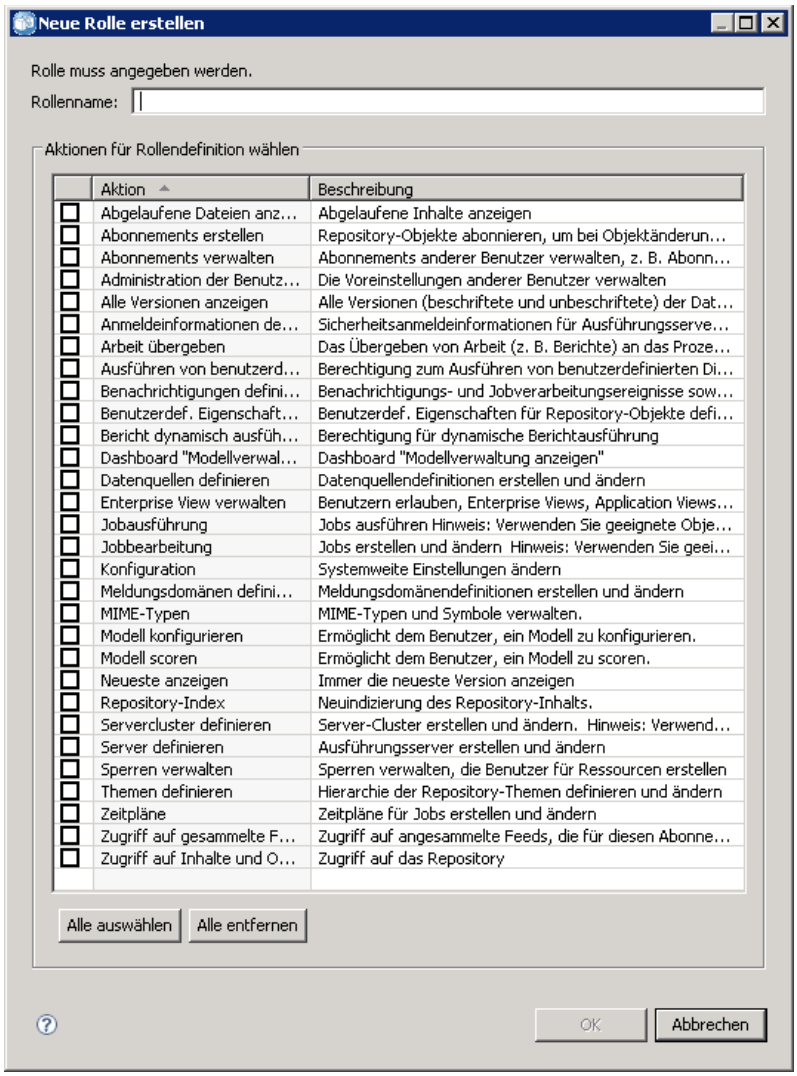
Definition von Rollen. Zeigt eine Liste der Aktionen, die mit einer ausgewählten Rolle assoziiert sind. Um die Aktionen zu bearbeiten, die mit einer ausgewählten Rolle verknüpft sind, klicken Sie auf die Schaltfläche Aktionen bearbeiten.

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.

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

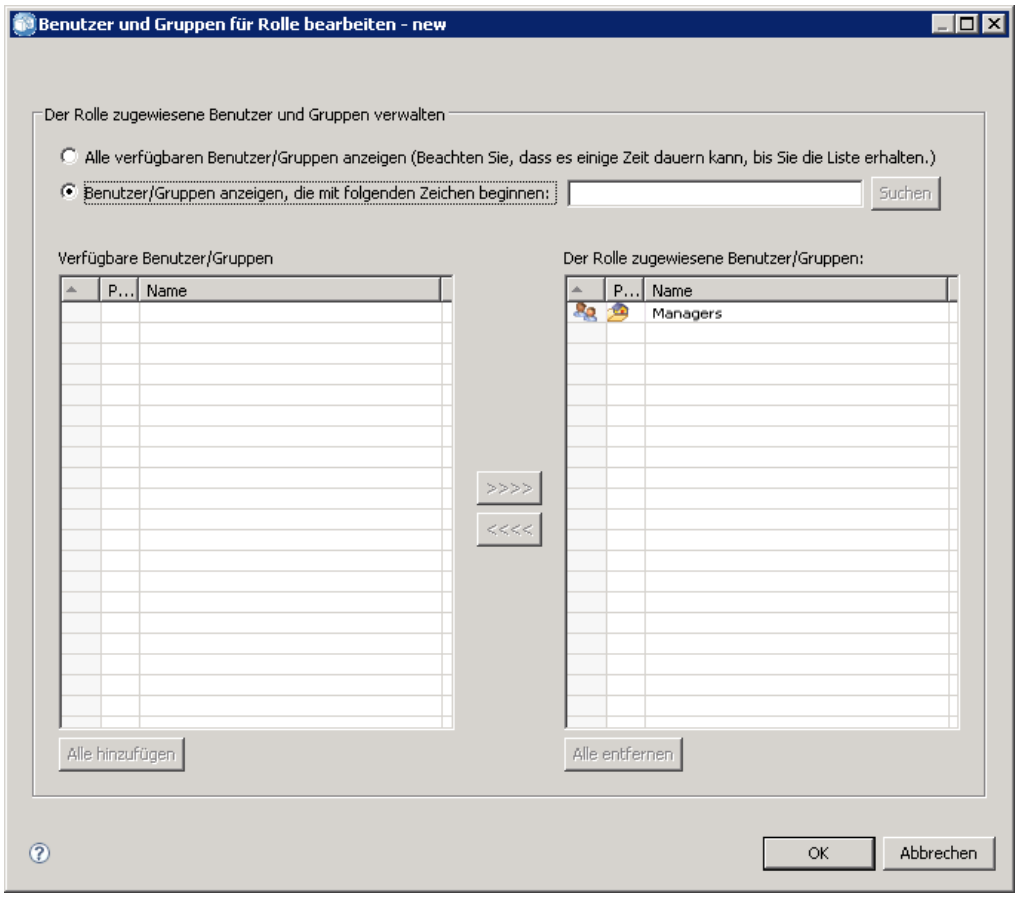
Aktion. Enthält alle Aktionen, die im System definiert und verfügbar sind. Anfangs sind mit einer Rolle keine Aktionen assoziiert.

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 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.

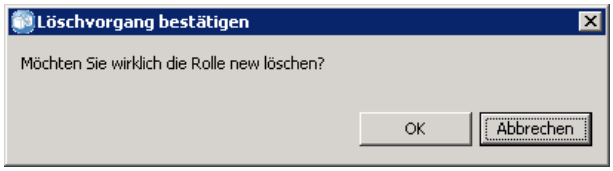
Die Liste "Verfügbare Benutzer/Gruppen" wird gemäß den Suchoption mit Benutzern und Gruppen gefüllt. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf die Schaltfläche >>>>, um ihn bwz. sie der Rolle zuzuweisen. Wenn Sie einen Benutzer oder eine Gruppe von einer Rolle entfernen möchten, 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.

Kapitel 6

XSS-Filter (Cross Site Scripting)

Cross Site Scripting (XSS) ist eine Computer-Sicherheitslücke, die häufig in Webanwendungen zu finden ist. Sie ermöglicht Angreifern, die clientseitigen Sicherheitsmechanismen zu umgehen, die normalerweise von modernen Webbrowsern für Webinhalte implementiert werden, indem sie ein schädliches Skript in von anderen Personen angezeigte Webseiten einbringt. Abhängig von der Sensibilität Ihrer Daten kann XSS ein erhebliches Sicherheitsrisiko darstellen.

In den Versionen von IBM® SPSS® Collaboration and Deployment Services vor 5 stand ein Websicherheitsfilter zur Verfügung, um XSS-Angriffe durch Validieren der von den Benutzern eingegebenen Parameter zu bekämpfen. Allerdings waren sämtliche Filterkriterien im Produkt eingebettet und konnten nicht von den Benutzern bearbeitet bzw. angepasst werden. Bei IBM® SPSS® Collaboration and Deployment Services Deployment Manager können die Benutzer nun XSS-Filterregeln entsprechend den in ihrem Unternehmen geltenden Sicherheitsrichtlinien hinzufügen, bearbeiten und löschen.

Verwalten von XSS-Filterregeln

Mit IBM® SPSS® Collaboration and Deployment Services Deployment Manager können Sie XSS-Filterregeln entsprechend den in Ihrem Unternehmen geltenden Sicherheitsrichtlinien verwalten. Um mit XSS-Filtern zu arbeiten, rufen Sie zunächst die administrative Schnittstelle auf:

1. Wählen Sie im Menü “Extras” die Option Server-Verwaltung.
2. Melden Sie sich in der Registerkarte “Server-Administration” bei einem Repository-Server an. Doppelklicken Sie auf das Symbol Konfiguration, um die Hierarchie zu erweitern.
3. Doppelklicken Sie auf das Symbol Cross-Site Scripting-Filter.

   Der Editor “Definitionen für XSS-Filterregeln verwalten” wird geöffnet.

   In diesem Editor werden alle derzeit für den Server definierten XSS-Filterregeln angezeigt. Administratoren können XSS-Filterregeln erstellen, ändern und löschen. Wählen Sie in der Dropdown-Liste einen Filtertyp aus, um alle Filterregeln anzuzeigen, die derzeit für diesen Typ definiert sind. Die folgenden Filtertypen stehen zur Verfügung:

   - HTML-Elemente einschränken
   - JavaScript-Funktionen einschränken
   - Strings mit einfachem Text einschränken
   - Reguläre Ausdrücke für Einschränkungsstring
   - Zulässige Strings

   Änderungen an XSS-Filterregeln werden sofort angewendet (kein Server-Neustart erforderlich).

Erstellen von XSS-Filterregeln

So erstellen Sie eine neue XSS-Filterregel:

1. Wählen Sie im Editor “Definitionen für XSS-Filterregeln verwalten” den Filtertyp aus, für den Sie eine neue Regel erstellen möchten.
2. Klicken Sie auf Hinzufügen. Das Dialogfeld “Regel bearbeiten” wird geöffnet.
3. Geben Sie den gewünschten Wert für die neue XSS-Filterregel ein und klicken Sie auf OK.

In dieser Dokumentation sind keine Beispiele für XSS-Filterregeln enthalten, da diese Anregungen für schädliche Skripts geben könnten.

Kapitel
7

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.
- **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. Im Gegensatz zum nativen Provider kann dieser Provider aktiviert und 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. Dieser Provider kann aktiviert oder 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 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 *ShowCase-Administratorhandbuch*.

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. Klicken Sie zur Konfiguration eines neuen Sicherheits-Providers mit der rechten Maustaste auf Sicherheits-Provider und wählen Sie die Option Neu. Ein Assistent wird angezeigt. Um die Konfiguration eines bestehenden Sicherheitsanbieters zu bearbeiten, doppelklicken Sie unter Sicherheits-Provider auf den Namen des betreffenden Sicherheits-Providers.

   Klicken Sie zum Aktivieren oder Deaktivieren von Sicherheits-Providern auf der Registerkarte “Server-Verwaltung” auf diese und wählen Sie Aktivieren bzw. Deaktivieren aus.

Abbildung 7-1
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. Details finden Sie in den folgenden Themen.

Klicken Sie zum Aktivieren oder Deaktivieren von Sicherheits-Providern auf der Registerkarte “Server-Verwaltung” auf diese und wählen Sie Aktivieren bzw. Deaktivieren aus.

Anmerkung: Wenn Änderungen an einer bereits bestehenden Sicherheits-Provider-Definition vorgenommen werden, werden diese erst aktiviert, nachdem das Repository neu gestartet oder der Sicherheitsprovider deaktiviert und erneut aktiviert wurde. In bestimmten Fällen, beispielsweise, wenn der Domänenname für den Active Directory-Sicherheits-Provider geändert wird, müssen

Benutzer und Gruppen entfernt und anschließend erneut bestimmten Rollen zugewiesen werden. Für weitere Informationen siehe Thema Einrichten von IBM SPSS Collaboration and Deployment Services-Benutzern in Kapitel 4 auf S. 25.

Native

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

OpenLDAP

Um eine bestehende OpenLDAP-Konfiguration zu bearbeiten, doppelklicken Sie unter Sicherheits-Provider auf den Eintrag OpenLDAP.

Klicken Sie zur Konfiguration eines neuen OpenLDAP-Sicherheits-Providers mit der rechten Maustaste auf Sicherheits-Provider und wählen Sie folgende Optionsfolge:
Neu > Sicherheits-Provider-Definition

Der Assistent zum Erstellen einer neuen Sicherheits-Provider-Definition wird angezeigt. Wählen Sie im Dropdown-Menü Typ die Option OpenLDAP. Geben Sie einen Namen für die Sicherheits-Provider-Definition ein, klicken Sie auf Weiter und arbeiten Sie die einzelnen Schritte im Assistenten ab. Beachten Sie die folgenden Details.

Host-Einstellungen

- **Host-URL.** Der Pfad zum LDAP-Server, in der Regel ein DNS-auflösbarer Name oder eine IP-Adresse (beispielsweise *ldap://IhrServer.IhrUnternehmen.com*). Der Standardport für LDAP ist 389.
- **Secured Socket Layer-Verbindung verwenden.** Wählen Sie die Verwendung von Secure Sockets für die Kommunikation mit dem OpenLDAP-Server.
- **Paging für Suchergebnisse.** Wählen Sie diese Option aus, wenn der LDAP-Server eine Option zum Paging von LDAP-Suchergebnissen aufweist (hierfür muss die Option aktiviert sein). Weitere Informationen zum Suchsteuerelement für Paging-Ergebnisse finden Sie unter *RFC 2686 - LDAP Control Extension for Simple Paged Results Manipulation* (*http://datatracker.ietf.org/doc/rfc2696/*).

Anmeldeinformationen

- **Typ der Such-Anmeldeinformationen.** Geben Sie an, wie mit den Such-Anmeldeinformationen umgegangen werden soll. Sofern dies laut Back-End-Server zulässig ist, haben Sie mit der Option *Anonyme Bindung verwenden* die Möglichkeit, nach Benutzern zu suchen, ohne eine Suchbenutzer-ID und ein Suchbenutzerpasswort angeben zu müssen. Bei der Option *Kerberos-Anmeldeinformation verwenden* wird die Anmeldeinformation für die Serververarbeitung des Servers für Suchvorgänge verwendet. Wählen Sie die Option *Bereitgestellte Anmeldeinformationen verwenden* aus, um eine Benutzer-ID und ein Kennwort als Anmeldeinformationen für die Suche anzugeben.

- **Suchbenutzer.** 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.
- **Suchbenutzerpasswort.** Aus Sicherheitsgründen wird das Passwort des Domänenbenutzers durch Sternchen (*) ersetzt. Geben Sie den Wert in beide Passwortfelder ein, um den korrekten Wert zu bestätigen.

Definition der Benutzerbindung

- **Kontext-Bindung verwenden.** Wählen Sie diese Option zum Durchführen einer Bindung aus, wenn sich der Benutzer anmeldet (wird empfohlen).
- **Passwortattribut.** Das zu verwendende Passwortattribut, wenn keine Benutzer-Bindung erwünscht ist. Bei Auswahl dieser Option bestätigen Sie, dass beim Sicherheitsserver in Abfragen ein Ergebniswert des Passwortattributs zulässig ist. Anderenfalls kann diese Option nicht verwendet werden.
- **Passwort-Digest.** Die Passwort-Digest-Methode, die vom Sicherheitsserver zum Hashing des Passworts verwendet wird. Diese Option wird verwendet, wenn keine Benutzer-Bindung erwünscht ist. Bei Auswahl dieser Option bestätigen Sie, dass beim Sicherheitsserver in Abfragen ein Ergebniswert des Passwortattributs zulässig ist. Anderenfalls kann diese Option nicht verwendet werden.

Einstellungen für die Benutzersuche

- **Basis-DN für Suchfilter.** Basis-**Distinguished-Name** für Benutzersuchen.
- **Objektfilterausdruck.** Objektklasse und -wert für die Filterung. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Suchfilterausdruck.** Das als Such-ID zu verwendende Attribut. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Suchfilterausdruck.** Das Attribut, das mit dem Attribut “Suchfilterausdruck” übereinstimmt. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Filter für Gruppenbenutzer.** Attribut, das die Benutzergruppenzugehörigkeit angibt.

Einstellungen für die Gruppensuche

- **Basis-DN für Suchfilter.** Basis-Distinguished-Name für Gruppensuchen.
- **Objektfilterausdruck.** Objektklasse und -wert für die Filterung. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Suchfilterausdruck.** Das als Such-ID zu verwendende Attribut. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Gruppenattribut.** Das Attribut, das mit dem Attribut “Suchfilterausdruck” übereinstimmt. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Mitgliedschaftsattribut.** Das Attribut, das die Gruppenzugehörigkeit angibt. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Aktualisierungsintervall.** Intervall, mit dem die Daten der Gruppenzugehörigkeit aktualisiert werden.

Active Directory

Klicken Sie zur Konfiguration eines neuen **Active Directory**-Sicherheits-Providers mit der rechten Maustaste auf Sicherheits-Provider und wählen Sie folgende Optionsfolge:
Neu > Sicherheits-Provider-Definition

Der Assistent zum Erstellen einer neuen Sicherheits-Provider-Definition wird angezeigt. Wählen Sie im Dropdown-Menü Typ die Option Active Directory. Geben Sie einen Namen für die Sicherheits-Provider-Definition ein, klicken Sie auf Weiter und arbeiten Sie die einzelnen Schritte im Assistenten ab. Beachten Sie die folgenden Details.

Host-Einstellungen

- **Host-URL.** URL für den Active Directory-Server. Der Standardport für LDAP ist 389.
- **Secured Socket Layer-Verbindung verwenden.** Wählen Sie die Verwendung von Secure Sockets für die Kommunikation mit dem Active Directory-Server.
- **Paging für Suchergebnisse.** Wählen Sie diese Option aus, wenn der Active Directory-Server eine Option zum Paging von Active Directory-Suchergebnissen aufweist (hierfür muss die Option aktiviert sein).

Anmeldeinformationen

- **Typ der Such-Anmeldeinformationen.** Geben Sie an, wie mit den Such-Anmeldeinformationen umgegangen werden soll. Sofern dies laut Back-End-Server zulässig ist, haben Sie mit der Option *Anonyme Bindung verwenden* die Möglichkeit, nach Benutzern zu suchen, ohne eine Suchbenutzer-ID und ein Suchbenutzerpasswort angeben zu müssen. Bei der Option *Kerberos-Anmeldeinformation verwenden* wird die Anmeldeinformation für die Serververarbeitung des Servers für Suchvorgänge verwendet. Wählen Sie die Option *Bereitgestellte Anmeldeinformationen verwenden* aus, um eine Benutzer-ID und ein Kennwort als Anmeldeinformationen für die Suche anzugeben.
- **Suchbenutzer.** 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.
- **Suchbenutzerpasswort.** Aus Sicherheitsgründen wird das Passwort des Domänenbenutzers durch Sternchen (*) ersetzt. Geben Sie den Wert in beide Passwortfelder ein, um den korrekten Wert zu bestätigen.

Domänenname.

- **Domäne.** Der DNS-Namespace, in dem sich der Benutzer anmeldet.

Definition der Benutzerbindung

- **Kontext-Bindung verwenden.** Wählen Sie diese Option zum Durchführen einer Bindung aus, wenn sich der Benutzer anmeldet (wird empfohlen).
- **Passwortattribut.** Das zu verwendende Passwortattribut, wenn keine Benutzer-Bindung erwünscht ist. Bei Auswahl dieser Option bestätigen Sie, dass beim Sicherheitsserver in Abfragen ein Ergebniswert des Passwortattributs zulässig ist. Anderenfalls kann diese Option nicht verwendet werden.

- **Passwort-Digest.** Die Passwort-Digest-Methode, die vom Sicherheitsserver zum Hashing des Passworts verwendet wird. Diese Option wird verwendet, wenn keine Benutzer-Bindung erwünscht ist. Bei Auswahl dieser Option bestätigen Sie, dass beim Sicherheitsserver in Abfragen ein Ergebniswert des Passwortattributs zulässig ist. Anderenfalls kann diese Option nicht verwendet werden.

Einstellungen für die Benutzersuche

- **Basis-DN für Suchfilter.** Basis-**Distinguished-Name** für Benutzersuchen.
- **Objektfilterausdruck.** Objektklasse und -wert für die Filterung. Dieser Wert hängt vom verwendeten Schema ab.
- **Suchfilterausdruck.** Das als Such-ID zu verwendende Attribut. Dieser Wert hängt vom verwendeten Schema ab.
- **Suchfilterausdruck.** Das Attribut, das mit dem Attribut "Suchfilterausdruck" übereinstimmt. Dieser Wert hängt vom verwendeten Schema ab.
- **Filter für Gruppenbenutzer.** Attribut, das die Benutzergruppenzugehörigkeit angibt.

Einstellungen für die Gruppensuche

- **Basis-DN für Suchfilter.** Basis-Distinguished-Name für Gruppensuchen.
- **Objektfilterausdruck.** Objektklasse und -wert für die Filterung. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Suchfilterausdruck.** Das als Such-ID zu verwendende Attribut. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Gruppenattribut.** Das Attribut, das mit dem Attribut "Suchfilterausdruck" übereinstimmt. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Mitgliedschaftsattribut.** Das Attribut, das die Gruppenzugehörigkeit angibt. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Aktualisierungsintervall.** Intervall, mit dem die Daten der Gruppenzugehörigkeit aktualisiert werden.

Active Directory mit lokaler Überschreibung

Klicken Sie zur Konfiguration eines neuen Sicherheits-Providers für ein Active Directory mit lokalem Überschreiben mit der rechten Maustaste auf Sicherheits-Provider und wählen Sie folgende Optionsfolge:
Neu > Sicherheits-Provider-Definition

Der Assistent zum Erstellen einer neuen Sicherheits-Provider-Definition wird angezeigt. Wählen Sie im Dropdown-Menü Typ die Option Active Directory mit lokalem Überschreiben. Geben Sie einen Namen für die Sicherheits-Provider-Definition ein, klicken Sie auf Weiter und arbeiten Sie die einzelnen Schritte im Assistenten ab.

Die meisten Einstellungen sind identisch mit denen für Active Directory. Jedoch bietet das lokale Überschreiben zwei zusätzliche Einstellungen:

- **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.

IBM i

Nach der Installation wird "IBM i" unter den Sicherheits-Providern in IBM® SPSS® Collaboration and Deployment Services Deployment Manager angezeigt. Geben Sie zur Konfiguration des IBM i-Sicherheits-Providers Werte für die folgenden Einstellungen an:

- **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 der `QSECOFR`-Ebene angeben, werden alle Profile im System ausgegeben. Wenn Sie einen Benutzer mit weniger Berechtigungen verwenden, werden basierend auf den Sicherheitseinstellungen der Benutzerprofile weniger Profile ausgegeben.

IBM i-Benutzer- und -Gruppenberechtigungen

Wenn ein IBM i-Benutzerprofil als Gruppe verwendet werden soll, müssen dem Profil andere IBM i-Profile 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* hingegeben *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-Anwendungsbenutzer

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

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.

So ändern Sie die verwendeten Sicherheits-Provider:

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

Beachten Sie, dass ausschließlich Sicherheits-Provider in der Liste angezeigt werden, die zuvor im IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Client erstellt wurden.

Aktivieren und Deaktivieren von Sicherheits-Providern

Es werden ausschließlich Sicherheits-Provider im Browser angezeigt, die zuvor im IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Client erstellt und konfiguriert wurden. Bei jedem Sicherheits-Providertyp können Sie einige Einstellungen anzeigen, die für die Art des eingesetzten Authentifizierungs- und Autorisierungssystems typisch sind. Verwenden Sie jedoch den Deployment Manager-Client, um neue Sicherheits-Provider zu konfigurieren oder die Einstellungen insgesamt zu ändern.

Sie können die verfügbaren Sicherheits-Provider mit den Kontrollkästchen neben jedem Sicherheits-Provider und durch Klicken auf Festlegen aktivieren bzw. deaktivieren.

Nativ (lokal)

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

Active Directory

Um bestimmte Active Directory-Einstellungen anzuzeigen, klicken Sie rechts neben dem Kontrollkästchen “Active Directory” auf Einstellungen anzeigen. Es wird eine Untergruppe der aktuellen Einstellungen angezeigt. Beachten Sie, dass der Active Directory-Sicherheits-Provider nur verfügbar ist, wenn dieser zuvor im IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Client konfiguriert wurde. Informationen zu speziellen Einstellungen finden Sie hier: Active Directory.

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 bestimmte Active Directory-Einstellungen mit lokalem Überschreiben anzuzeigen, klicken Sie rechts neben dem Kontrollkästchen “Active Directory mit lokalem Überschreiben” auf Einstellungen anzeigen. Es wird eine Untergruppe der aktuellen Einstellungen angezeigt. Die meisten Einstellungen entsprechen denen für Active Directory. Darüber hinaus stehen jedoch die beiden folgenden Optionen zur Verfügung. Beachten Sie, dass der Active Directory-Sicherheits-Provider mit lokalem Überschreiben nur verfügbar ist, wenn dieser zuvor im IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Client konfiguriert wurde.

- **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.

IBM i

Wenn das IBM® SPSS® Collaboration and Deployment Services Repository auf IBM i installiert ist, wird das IBM i-Benutzerprofilverzeichnis verwendet, um Repository-Anmeldungen zu authentifizieren. Um bestimmte IBM i-Einstellungen anzuzeigen, klicken Sie rechts neben dem Kontrollkästchen “IBM i” auf Einstellungen anzeigen. Es wird eine Untergruppe der aktuellen Einstellungen angezeigt. Beachten Sie, dass der IBM i-Sicherheits-Provider nur verfügbar ist, wenn dieser zuvor im IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Client installiert und konfiguriert wurde.

- **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 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 der QSECOFR-Ebene angeben, werden alle Profile im System ausgegeben. Wenn Sie einen Benutzer mit weniger Berechtigungen verwenden, werden basierend auf den Sicherheitseinstellungen der Benutzerprofile weniger Profile zurückgegen.

OpenLDAP

Um bestimmte OpenLDAP-Einstellungen anzuzeigen, klicken Sie rechts neben dem Kontrollkästchen “OpenLDAP” auf Einstellungen anzeigen. Es wird eine Untergruppe der aktuellen Einstellungen angezeigt. Beachten Sie, dass der OpenLDAP-Sicherheits-Provider nur verfügbar ist, wenn dieser zuvor im IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Client konfiguriert wurde. Informationen zu speziellen Einstellungen finden Sie hier: OpenLDAP.

Kapitel
8

Einzelanmeldung

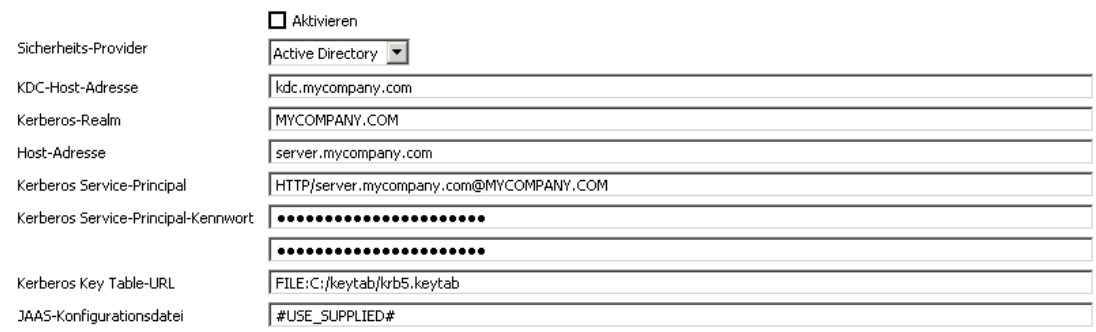
Einzelanmeldung (SSO) ist eine Methode für die Zugriffskontrolle, die es einem Benutzer ermöglicht, sich einmal anzumelden und Zugriff auf Ressourcen mehrerer Softwaresysteme zu erhalten, ohne sich mehrmals anmelden zu müssen. IBM® SPSS® Collaboration and Deployment Services bietet die Möglichkeit der 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 8-1
Editor für Einzelanmeldungs-Provider



- **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.

Kapitel
9

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.
- 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 IBM Corp.-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 9-1
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 Berichtausgabe 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 und alle erforderlichen Komponenten müssen im Verzeichnis *<IBM SPSS Collaboration and Deployment Services-Installationsverzeichnis>/components/cache-provider* abgelegt 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 *Multicast-Gruppenadresse* und *Multicast-Gruppenport*, um die Standards zu überschreiben.	Standardmäßig deaktiviert.

Coordinator of Processes

Die Konfigurationsoptionen des Prozesskoordinators (Coordinator of Processes) ermöglichen Ihnen die Angabe von Einstellungen, die das Ablaufzeitlimit für Verbindungsanforderungen und Wartungsaktivitäten für den Coordinator of Processes beeinflussen. Um die Einstellungen zu bearbeiten, klicken Sie in der Konfigurationsliste unter "Prozesskoordinator" auf die entsprechende Option. In der folgenden Tabelle finden Sie Linknamen, Beschreibungen sowie gültige Einstellungen.

Tabelle 9-2
Konfigurationsoptionen für den Prozesskoordinator (Coordinator of Processes)

Name	Beschreibung	Einstellungen
Zeitüberschreitung für anstehende Verbindung	Das Ablaufzeitlimit für anstehende Verbindungsanforderungen. Der Prozesskoordinator (Coordinator of Processes) verwirft eine Verbindungsanforderung, wenn der Zielserver nicht innerhalb des angegebenen Zeitintervalls antwortet.	Ganzzahl. Die Standardeinstellung lautet 5 (Sekunden).
Wartungs-Provider für Prozesskoordinator aktiviert	Aktiviert bzw. deaktiviert Wartungsaktivitäten für den Prozesskoordinator	Standardmäßig aktiviert.

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 9-3
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 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 Repositorys 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 spsscr:///?id=0a30063bc975ede400. Den URI finden Sie in den Objekteigenschaften. Weitere Informationen finden Sie in der IBM® SPSS® Collaboration and Deployment Services Deployment Manager-Dokumentation.

Name	Beschreibung	Einstellungen
SPSS Statistics-Serveranmeldedaten	Die Anmeldeinformationen, über die eine Verbindung mit dem SPSS Statistics-Server hergestellt wird, wenn Syntax für ein benutzerdefiniertes Dialogfeld ausgeführt wird. *Hinweis*: 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 9-4
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 9-5
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 *com.spss.er.internal.configuration.ConfiguredAuthenticationImpl* und die Einstellung wird im Klassenpfad des Anwendungsservers vorgenommen. Die Klasse muss der Authentifizierungsschnittstelle entsprechen, die von Deployment Portal bereitgestellt wird (*com.spss.er.internal.configuration.ConfiguredAuthenticationInterface.java*).	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 9-6
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 Strichpunkte 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	Standardmäßig aktiviert.

Name	Beschreibung	Einstellungen
	Statistics-Datendatei-Server angegeben werden.	
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-Konfigurationsoptionen ermöglichen es Ihnen, den Speicherort der Dokumentationskomponenten für das browserbasierte IBM® SPSS® Collaboration and Deployment Services Deployment Manager anzugeben. Standardmäßig verwendet das System die vom Installationsprogramm festgelegten Pfade. In der Tabelle Hilfe sind die verfügbaren Einstellungen beschrieben.

Tabelle 9-7
Konfigurationsoptionen für die Hilfe

Name	Beschreibung	Einstellungen
Handbuchverzeichnis	Gibt den Speicherort der IBM® SPSS® Collaboration and Deployment Services-Handbücher an.	Der Pfad zu dem Verzeichnis, das die Handbücher enthält.
Hilfeverzeichnis	Gibt den Speicherort des Hilfesystems für Deployment Manager an.	Der Pfad zu dem Verzeichnis, das das Hilfesystem enthält.

Führen Sie zum Ändern einer Hilfeeinstellung folgende Schritte aus:

1. Klicken Sie in der Konfigurationsliste auf die Einstellung, die in der Gruppe Hilfe geändert werden soll. Der aktuelle Wert wird angezeigt.
2. Geben Sie den neuen Wert ein.
3. Klicken Sie auf Setzen. Der von Ihnen angegebene Wert wird als aktueller Wert für die betreffende Einstellung 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.

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 13 auf S. 114. 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 9-8
Konfigurationsoptionen für Benachrichtigungen

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

Name	Beschreibung	Einstellungen
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.
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”.

Name	Beschreibung	Einstellungen
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 ist 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. Die Standardeinstellung lautet DISK.
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”.

Name	Beschreibung	Einstellungen
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.
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 Befehl EHLO 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 *InetAddress.getLocalHost().getHostName()*. 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.

Name	Beschreibung	Einstellungen
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.
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 *SendFailedException* 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.
SMPT - 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.

Name	Beschreibung	Einstellungen
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.
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 Repositorys 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 9-9
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.
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. Beispielsweiseist die Naming-Factory für den JBoss-Anwendungsserver *org.jnp.interfaces.Naming-ContextFactory*. 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. Beispielsweiselautet die Naming-Factory für den JBoss-Anwendungsserver jnp://localhost:1099.. 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.
Obergrenze für Jobverlauf	Maximale Anzahl an Jobverlaufseinträgen, die für jede Version eines Jobs gespeichert werden sollen. Wenn die Obergrenze erreicht ist, werden die ältesten Jobverlaufseinträge durch neuere Einträge ersetzt.	Ganzzahl. Die Standardeinstellung lautet 10.
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. Die Standardeinstellung lautet “wahr”.
Abgelaufene übergebene Artefakte entfernen	Gibt an, ob Artefakte, die durch die Übergabe einer Ressource für die Verarbeitung erstellt wurden, bei ihrem Ablauf aus dem Repository entfernt werden sollen.	Standardmäßig aktiviert.
Veraltete Jobverläufe entfernen	Gibt an, ob veraltete Jobverläufe entfernt werden sollen.	Standardmäßig aktiviert.

Name	Beschreibung	Einstellungen
Ablaufzeit für übergebenes Artefakt	Die Ablaufzeit (in Tagen) für übergebene Artefakte, wie beispielsweise Jobs.	Ganzzahl. Die Standardeinstellung lautet 5.
Zeitstempel für übergebenes Artefakt	Das Zeitstempelformat, das in den Namen von automatisch generierten Ordnern für übergebene Arbeiten verwendet werden soll.	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 9-10
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.
Anmeldepasswörter müssen verschlüsselt sein	Anmeldepasswörter müssen verschlüsselt sein. "Falsch" gibt an, dass Passwörter als unverschlüsselter Text übergeben werden dürfen. *Anmerkung:* 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 Anmeldepasswörter 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.

Name	Beschreibung	Einstellungen
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.
Objekt-Caching: Enable	Gibt an, ob das Caching von Repository-Objekten aktiviert ist oder nicht. Bei Auswahl dieser Option müssen Sie entweder den internen Cache aktivieren oder die Einstellungen für einen externen Cache angeben.	Standardmäßig deaktiviert.
Objekt-Caching: Adresse des externen Cache	Adresse für den externen Cache. Wird nur benötigt, wenn der interne Cache nicht verwendet wird.	Gültige Netzwerkadresse.
Objekt-Caching: Port für externen Cache	Portnummer für den externen Cache. Wird nur benötigt, wenn der interne Cache nicht verwendet wird.	Gültige Portnummer.
Objekt-Caching: Internen verwenden	Gibt an, ob der interne Cache verwendet werden soll.	Standardmäßig deaktiviert.
Größe der Wartenschlange neu indizieren	Definiert die Größe der Warteschlange, die für die Neuindizierung des Repositorys 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 Repositorys verwendet werden.	Ganzzahl. Die Standardeinstellung lautet 5.
Gelöschte Ressourcen entfernen	Gibt an, ob gelöschte Elemente aus dem Repository entfernt werden sollen. Diese Option sollte immer aktiviert sein. Sie sollte nur in Sonderfällen (z. B. zu Debugging-Zwecken) deaktiviert werden.	Standardmäßig aktiviert.
Repository-Wartung aktiviert	Aktiviert bzw. deaktiviert den Wartungsdienst für das Repository.	Wahr oder Falsch. Die Standardeinstellung lautet “Wahr”.
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.

Name	Beschreibung	Einstellungen
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 *[JJJJ-MM-TT] HH:MM:SS*.
Beginn der Repository-Wartung (Max.)	Legt die maximale Verzögerungszeit für den Start des Wartungsdiensts fest.	Ganzzahl. Die Standardeinstellung lautet 30 Minuten.
Beginn der Repository-Wartung (Min.)	Legt die Mindestverzögerungszeit für den Start des Wartungsdiensts fest.	Ganzzahl. Die Standardeinstellung lautet 5 Minuten.
Transaktionsverzögerung für Repository-Wartung	Gibt den Prozentsatz der Verzögerungszeit an der Wartungseinheit bzw. Arbeit insgesamt an. Wenn die Transaktionsverzögerung für die Wartung beispielsweise 75 Prozent (Standard) beträgt und die Transaktion 1 Sekunde dauerte, folgt darauf eine 3-sekündige Verzögerung.	Ganzzahl zwischen 1 und 99. Die Standardeinstellung lautet 75.
Transaktionsdauer für Repository-Wartung	Gibt die Dauer der einzelnen Wartungstransaktionen (in Millisekunden)n 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.	Ganzzahl. Die Standardeinstellung lautet 500 Millisekunden. Negative Werte werden als "ohne Begrenzung" interpretiert.
Repository-Benachrichtigung aktiviert	Gibt an, ob der Repository-Server mit dem Benachrichtigungsserver kommunizieren soll.	Standardmäßig deaktiviert.

Name	Beschreibung	Einstellungen
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	Zuordnungsimplementierung für ID-Suche beim Übertragen von Ressourcen.	DISK oder MEMORY.
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 9-11
Scoring-Service-Konfigurationsoptionen

Name	Beschreibung	Einstellungen
Audit-Zeitabstand	Die Zahl der Millisekunden zwischen Audit-Aktualisierungen.	Ganzzahl. Die Standardeinstellung lautet 3600000.
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 9-12
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 15 auf S. 123. Beachten Sie, dass das Aktivieren dieser Option die Suchfunktion verlangsamen kann.	Standardmäßig deaktiviert.
Standard-Seitengröße	Anzahl der Suchergebnisse, die auf einer Seite angezeigt werden.	Ganzzahl. Die Standardeinstellung lautet 25.

Name	Beschreibung	Einstellungen
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.
Suchdienstwartung aktiviert	Gibt an, ob Wartungsaktivitäten für den Suchdienst aktiviert sind.	Standardmäßig aktiviert.

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 9-13
Sicherheitskonfigurationsoptionen

Name	Beschreibung	Einstellungen
Dauer der Kontosperre	Anzahl an Minuten bis zur automatischen Aufhebung der Sperre eines Benutzers, der gesperrt worden war, nachdem er die zulässige Anzahl an ungültigen Anmeldeversuchen überschritten hatte.	Ganzzahl. Die Standardeinstellung lautet 30. Der Wert 0 bedeutet, dass Benutzersperren niemals automatisch aufgehoben werden.
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.

Name	Beschreibung	Einstellungen
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.
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.
Zählerschwellenwert für ungültige Anmeldeversuche	Anzahl der fehlgeschlagenen Anmeldeversuche, bevor der Benutzer automatisch gesperrt wird.	Ganzzahl. Die Standardeinstellung lautet 3. Der Wert 0 bedeutet, dass Benutzer niemals automatisch gesperrt werden.
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 (*Normalisierungsform C* 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 9-14
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 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 *https* anstelle von *http* beginnen. Außerdem kann der Port weggelassen werden, wenn der Server den Standard-*http*-Port 80 oder den Standard-*https*-Port 443 verwendet. Der Server muss	URL.

Name	Beschreibung	Einstellungen
	neu gestartet werden, damit Änderungen am Präfix wirksam werden.	

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

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

Tabelle 9-15
IBM ShowCase-Konfigurationsoptionen

Name	Beschreibung	Einstellungen
Warehouse Builder-Datenbank	Der Name der Datenbank/Bibliothek für das Warehouse Builder-Set und Definitionsinformationen.	Gültiger Datenbank-/Bibliotheksname.
Warehouse Builder-Hostname	Die IP-Adresse bzw. der Hostname des IBM i-Servers, der von Warehouse Builder verwendet wird.	Eine gültige IP-Adresse bzw. ein gültiger Hostname.
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.
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 9-16
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)`

Kapitel
10

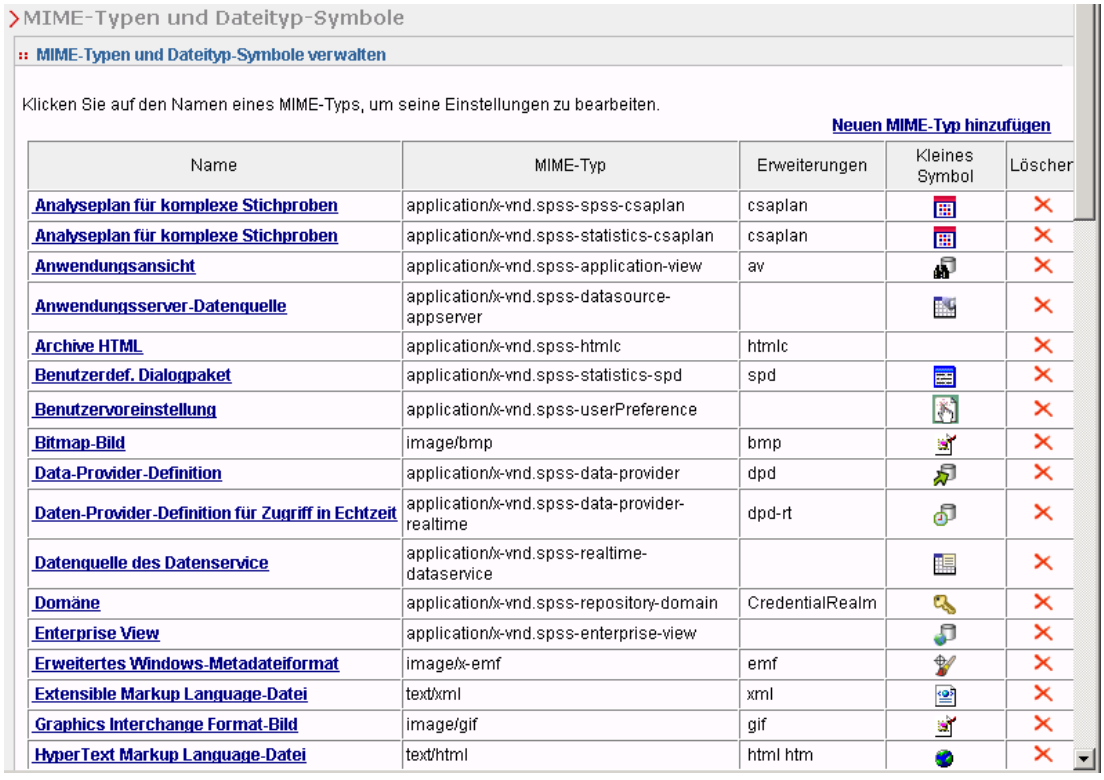
MIME-Typen

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 Dateiendungen 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 10-1
Seite "MIME-Typen und Dateityp-Symbole"



Name	MIME-Typ	Erweiterungen	Kleines Symbol	Löscher
Analyseplan für komplexe Stichproben	application/x-vnd.spss-spss-csaplan	csaplan		
Analyseplan für komplexe Stichproben	application/x-vnd.spss-statistics-csaplan	csaplan		
Anwendungsansicht	application/x-vnd.spss-application-view	av		
Anwendungsserver-Datenquelle	application/x-vnd.spss-datasource-appserver			
Archive HTML	application/x-vnd.spss-htmlc	htmlc		
Benutzerdef. Dialogpaket	application/x-vnd.spss-statistics-spd	spd		
Benutzervoreinstellung	application/x-vnd.spss-userPreference			
Bitmap-Bild	image/bmp	bmp		
Data-Provider-Definition	application/x-vnd.spss-data-provider	dpd		
Daten-Provider-Definition für Zugriff in Echtzeit	application/x-vnd.spss-data-provider-realtime	dpd-rt		
Datenquelle des Datenservice	application/x-vnd.spss-realtime-dataservice			
Domäne	application/x-vnd.spss-repository-domain	CredentialRealm		
Enterprise View	application/x-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		
HyperText 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. 91.

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.

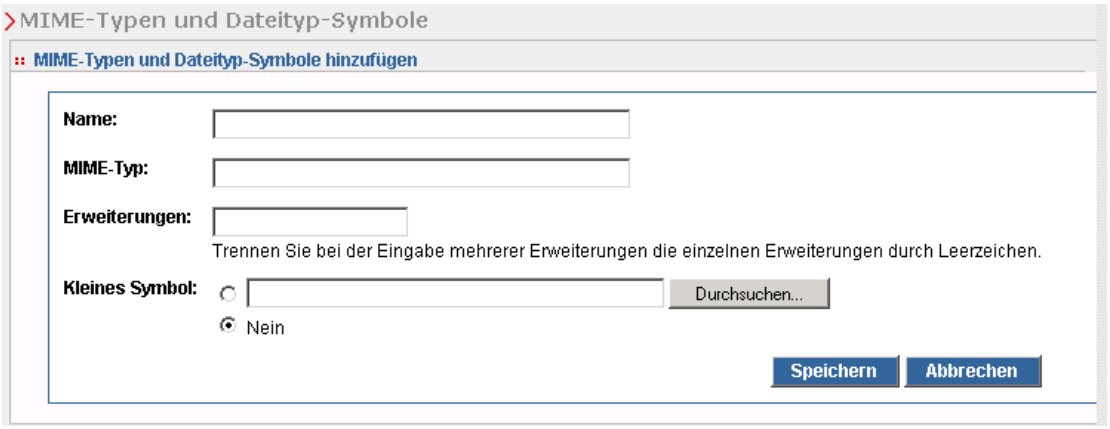
Untertypen enthalten häufig Präfixe, um MIME-Typen für spezifische Produkte zu kennzeichnen. Untertypen, die sich auf kommerzielle Produkte beziehen, enthalten zum Beispiel das Präfix *vnd.*, das einen Hersteller-Untertyp angibt, z. B.*application/vnd.ms-access*. Im Gegensatz dazu beinhalten Untertypen 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 10-2
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 Dateiendungen ein, die mit dem MIME-Typ verbunden werden sollen. Setzen Sie zwischen Einträgen ein Leerzeichen, wenn Sie mehrere Dateiendungen 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.

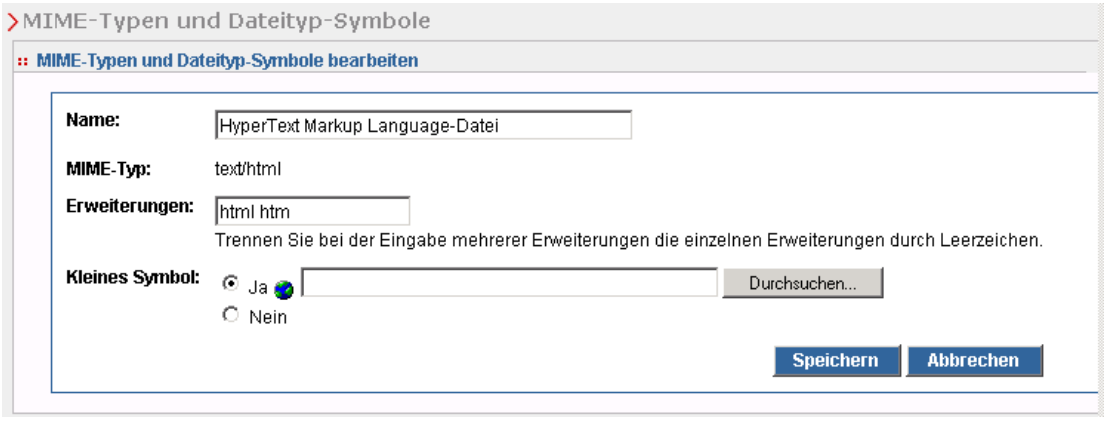
- Klicken Sie auf Speichern, um den MIME-Typ hinzuzufügen und zur Seite "MIME-Typen und Dateityp-Symbole hinzufügen" zurückzukehren, oder auf Abbrechen, um zurückzukehren, ohne den MIME-Typ auf dem Server zu speichern.

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 10-3
Bearbeiten von MIME-Typen



- 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.

Kapitel
11

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 9 auf S. 77. Die Repository-Suche wird automatisch deaktiviert, während die Neuinidizierung beim Start läuft.

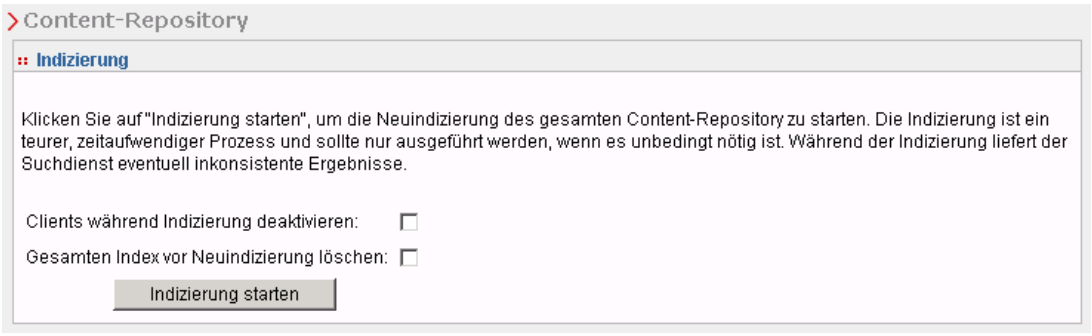
Eine Neuinidizierung kann auch im browserbasierten IBM® SPSS® Collaboration and Deployment Services Deployment Manager auf Anforderung eines autorisierten Benutzers durchgeführt werden. Für weitere Informationen siehe Thema Aktionen in Kapitel 5 auf S. 41.

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.

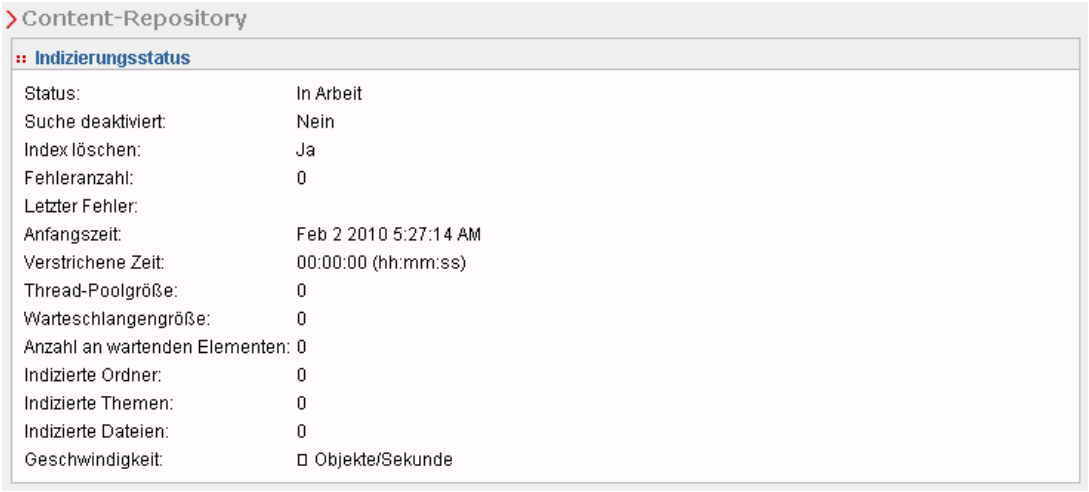
Abbildung 11-1
Indizierung des Content-Repository



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 11-2
Indizierungsstatus des Content-Repository



Kapitel
12

Repository-Wartung

Zur IBM® SPSS® Collaboration and Deployment Services Repository-Wartung können Aufgaben gehören wie die Sicherung bestehender Daten und Anwendungseinstellungen sowie die Bereinigung nicht verwendeter und veralteter Daten zur Gewährleistung von Datenintegrität und optimaler Leistung.

Im Laufe der Zeit nimmt für gewöhnlich die Größe des IBM SPSS Collaboration and Deployment Services Repository zu. Bei jedem Speichern eines Objekts wird eine neue Objektversion gespeichert. Außerdem sammeln sich Artefakte an, die bei jeder Jobausführung erstellt werden. Durch diesen Zustrom an Objekten und Versionen kann die Repository-Datenbank auf eine Größe anwachsen, die sich negativ auf die Leistungsfähigkeit auswirken kann. Die Leistungsverschlechterung kann zu einem erhöhten Zeitbedarf beim Speichern von Dateien führen. In Extremsituationen kann der Start von Operationen deutlich länger dauern als früher und sie können eventuell sogar aufgrund einer Zeitüberschreitung fehlschlagen. Um derartige Probleme zu vermeiden, sollten regelmäßig unnötige Objekte und Versionen entfernt werden.

Kandidaten für eine Entfernung sind folgende Elemente:

- Unbezeichnete Versionen von Objekten, die nicht benötigt werden
- Nicht benötigte Enterprise-Ansicht-Versionen
- Unnötige Job-Artefakte
- Abgelaufene übergebene Arbeiten Für weitere Informationen siehe Thema Entfernen abgelaufener übergebener Arbeiten auf S. 98.
- Alte Jobverläufe Für weitere Informationen siehe Thema Verwalten der Größe des Jobverlaufs auf S. 99.

Das Löschen nicht benötigter Elemente kann auf verschiedene Weisen erreicht werden. Sie können jedes Element einzeln identifizieren und entfernen. Alternativ können Sie mit dem Bereinigungsdienstprogramm Elemente, die angegebene Kriterien erfüllen, in einem Batch-Vorgang löschen. Abschließend können Sie IBM® SPSS® Collaboration and Deployment Services - Essentials for Python verwenden, um automatisierte Löschaufgaben zu erstellen, die zur Ausführung in regelmäßigen Abständen geplant werden können. Um zu verhindern, dass das Löschen einer großen Anzahl an Elementen die Gesamtleistung des Systems beeinträchtigt, wird der Löschvorgang von einem Wartungsdienst verwaltet.

Repository-Sicherung

Die IBM® SPSS® Collaboration and Deployment Services Repository-Daten und die Anwendungseinstellungen sind in einer relationalen Datenbank gespeichert und die Sicherung des Repositorys muss auf der Datenbankebene mit Sicherungsdienstprogrammen des Datenbankherstellers erfolgen. Es wird empfohlen, die Datenbank täglich zu sichern. Falls

erforderlich, kann das Repository über einer Sicherungskopie der Datenbank erneut installiert werden.

Automatischer Wartungsdienst

Beim Löschen von Elementen steht das Element mit sofortiger Wirkung für keinen IBM® SPSS® Collaboration and Deployment Services Repository-Client mehr zur Verfügung. Das Element wird zu diesem Zeitpunkt jedoch nicht entfernt, sondern lediglich für die Löschung gekennzeichnet. Die eigentliche Löschung wird durch einen Wartungsdienst durchgeführt. Dieser Dienst wird in regelmäßigen Abständen aktiviert und entfernt gekennzeichnete Elemente aus dem System. Wenn nicht alle gekennzeichneten Elemente im aktuellen Wartungsfenster entfernt werden können, bleiben die betreffenden Elemente bis zur nächsten Aktivierung des Diensts im System. Der Wartungsdienst minimiert die Auswirkungen von Löschvorgängen auf die Systemverarbeitung insgesamt.

Es gibt einige Ausnahmen, bei denen Elemente sofort entfernt und nicht nur gekennzeichnet werden. Wenn Sie eine Menge an Objektversionen löschen, die die Version *NEUESTER* enthält, wird die gesamte Menge sofort gelöscht, um die ordnungsgemäße Zuordnung des Labels *NEUESTER* zu einer neuen Version zu ermöglichen. Außerdem erzwingt die Durchführung eines Exportvorgangs das sofortige Löschen aller gekennzeichneten Versionen, um zu verhindern, dass gelöschte Elemente in das Exportset aufgenommen werden.

Konfigurieren der automatischen Repository-Wartung

Der Wartungsdienst führt eine Reihe von Aufgaben durch, unter anderem:

- Löschen von gekennzeichneten Objekten und Versionen
- Löschen veralteter Suchindizes
- Löschen veralteter Jobverläufe
- Entfernen abgelaufener übergebener Artefakte
- Entfernen abgelaufener anstehender Serververbindungen
- Entfernen von temporären Dateien, die während Export-, Import- und Höherstufungsaktivitäten erstellt wurden

Der Dienst wird gemäß einem Zeitplan ausgeführt, der durch eine Reihe von Konfigurationsparametern definiert wird. Werte für diese Parameter können Sie über den browserbasierten IBM® SPSS® Collaboration and Deployment Services Deployment Manager angeben. Alle Parameter stehen in der Gruppe “Repository” auf der Seite “Konfiguration” zur Verfügung.

1. Wählen Sie die Option Anfangsdatum für Repository-Wartung aus. Geben Sie einen Wert ein, der das Datum und die Uhrzeit für den Start des Wartungsdiensts angibt. Klicken Sie auf Setzen.
2. Wählen Sie die Option Beginn der Repository-Wartung (Max.) aus. Geben Sie einen Wert ein, der den längsten Zeitraum nach der festgelegten Startzeit angibt, zu der der Wartungsdienst gestartet werden sollte. Wenn der Dienst zum festgelegten Zeitpunkt nicht gestartet werden kann, ist

dieser Wert die maximale Zeitdauer, während derer versucht wird, den Dienst zu starten. Klicken Sie auf Setzen.

3. Wählen Sie die Option Beginn der Repository-Wartung (Min.) aus. Geben Sie einen Wert ein, der den kürzesten Zeitraum nach der festgelegten Startzeit angibt, zu der der Wartungsdienst gestartet werden sollte. Wenn der Dienst zum festgelegten Zeitpunkt nicht gestartet werden kann, ist dieser Wert die minimale Zeitdauer, während derer versucht wird, den Dienst zu starten. Klicken Sie auf Setzen.

4. Wählen Sie die Option Wartungshäufigkeit für Repository aus. Geben Sie einen Wert ein, der die Häufigkeit für die Ausführung des Wartungsdiensts angibt. Beispielsweise wird beim Wert 90 der Dienst alle 90 Minuten ausgeführt. Klicken Sie auf Setzen.

5. Wählen Sie die Option Transaktionsverzögerung für Repository-Wartung aus. Die Gesamtzeitdauer für eine Wartungstransaktion besteht aus der eigentlichen Wartungsarbeit zuzüglich einer Verzögerung, bevor die nächste Transaktion verarbeitet wird. Durch die Verzögerung kann sich das System anderen Aufgaben zuwenden, während der Wartungsdienst ausgeführt wird. Geben Sie einen Wert ein, der angibt, welcher Prozentsatz der Gesamtzeit für eine Wartungstransaktion dieser Verzögerung zugeteilt wird. Ein Wert von 50 % beispielsweise gibt an, dass auf die Transaktionsarbeit eine Verzögerung folgen soll, die genauso lange dauert, wie die Ausführung der Arbeit dauerte. Anders ausgedrückt: Auf die Verzögerung entfällt die Hälfte der Gesamtzeit für die Wartungstransaktion. Klicken Sie auf Setzen.

6. Wählen Sie die Option Transaktionsdauer für Repository-Wartung aus. Geben Sie einen Wert für die für eine Wartungstransaktion zugeteilte Zeit an. Klicken Sie auf Setzen.

7. Wenn Ihr IBM® SPSS® Collaboration and Deployment Services-Server in einer Cluster-Umgebung ausgeführt wird, haben Sie die Wahl, ob der Wartungsdienst auf allen Cluster-Knoten oder nur auf dem Master-Knoten ausgeführt werden soll. Wählen Sie in der Konfigurationsliste die Option Repository-Wartung – Master aus. Durch Auswahl dieser Option wird der Dienst auf den Master-Knoten beschränkt. Klicken Sie auf Setzen.

8. Führen Sie einen Neustart des IBM SPSS Collaboration and Deployment Services-Servers durch, um mit der Verwendung der neuen Einstellungen zu beginnen.

Weitere Informationen zu diesen Konfigurationseinstellungen finden Sie unter Repository.

Entfernen abgelaufener übergebener Arbeiten

Die im Ordner “Übergebene Jobs” erstellten Artefakte laufen automatisch nach einer bestimmten Anzahl von Tagen ab, wodurch sie nur noch für den Eigentümer und für Administratoren sichtbar sind. Wenn abgelaufene Artefakte nach dem Ablaufdatum nicht mehr benötigt werden, können Sie das System so konfigurieren, dass die Artefakte beim Ablauf automatisch für die Löschung gekennzeichnet werden. Bei der Aktivierung des Wartungsdiensts werden die Elemente aus dem Repository entfernt.

Sie können diese Funktion auf der Seite “Konfiguration” im browserbasierten IBM® SPSS® Collaboration and Deployment Services Deployment Manager steuern.

1. Wählen Sie die Option Abgelaufene übergebene Artefakte entfernen aus der Gruppe “Prozessmanagement” aus.

2. Durch Aktivieren des Kontrollkästchens können Sie diese Funktion aktivieren.

3. Klicken Sie auf Setzen.

Weitere Informationen zu dieser Konfigurationseinstellung finden Sie unter Prozessmanagement.

Verwalten der Größe des Jobverlaufs

Bei jeder Ausführung eines Jobs wird ein Eintrag zum Jobverlauf hinzugefügt, der detaillierte Informationen zur Ausführung dieses Jobs angibt, beispielsweise wann die Ausführung erfolgte und wie der Gesamtstatus der Ausführung lautete. Diese Einträge beinhalten auch Verweise auf die Jobausgabe und auf das Ausführungsprotokoll. Wenn ein Job gemäß einem Zeitplan ausgeführt wird, führt jede durch den Zeitplan initiierte Ausführung zu einem entsprechenden Eintrag im Jobverlauf.

Dadurch, dass jede Jobausführung einen Eintrag im Jobverlauf erzeugt, kann die Menge der im Jobverlauf verwalteten Informationen im Lauf der Zeit recht groß werden. Einige dieser Verlaufseinträge werden jedoch möglicherweise gar nicht benötigt. Verlaufseinträge für ältere Ausführungen eines Jobs sind häufig veraltet, sobald neuere Ausführungen des Jobs verfügbar sind. Zur Begrenzung der Größe des Jobverlaufs können Sie eine Obergrenze für die Anzahl der Jobverlaufseinträge festlegen, die für eine Jobversion beibehalten werden sollen. Wenn der Verlauf für eine Jobversion diese Obergrenze überschreitet, ist der älteste Verlaufseintrag veraltet und wird entfernt, wenn der Wartungsdienst aktiviert wird. Bei einer Obergrenze von 15 für die Größe des Jobverlaufs beispielsweise führt die 16. Ausführung dazu, dass der erste Verlaufseintrag entfernt wird.

Sie können diese Funktion auf der Seite “Konfiguration” im browserbasierten IBM® SPSS® Collaboration and Deployment Services Deployment Manager steuern. Zur automatischen Verwaltung der Jobverlaufseinträge führen Sie folgende Schritte aus:

1. Wählen Sie die Option Obergrenze für Jobverlauf aus der Gruppe “Prozessmanagement” aus. Geben Sie die Anzahl der Jobverlaufseinträge ein, die für jede Jobversion beibehalten werden sollen. Klicken Sie auf Setzen.

2. Wählen Sie die Option Veraltete Jobverläufe entfernen aus der Gruppe “Prozessmanagement” aus. Aktivieren Sie das Kontrollkästchen, um festzulegen, dass die ältesten Jobversionsverläufe entfernt werden sollen, die die Obergrenze für den Jobverlauf überschreiten. Klicken Sie auf Setzen.

Weitere Informationen zu diesen Konfigurationseinstellungen finden Sie unter Prozessmanagement.

Überwachen von Wartungsaktivitäten

Zusammenfassungen über die Aktivitäten des Wartungsdiensts können in die Systemprotokolldateien aufgenommen werden. Dadurch können Sie ermitteln, welche Aufgaben bei der Aktivierung des Diensts durchgeführt werden. So aktivieren Sie die Protokollierung für den Wartungsdienst:

1. Öffnen Sie die Konfigurationsdatei *log4j.xml* in einem Texteditor.
2. Suchen Sie das Kategorieelement für den Logger *com.spss.process.internal.maintenance*.
3. Setzen Sie die Protokolltiefe für diesen Logger auf *DEBUG*.
4. Speichern Sie Ihre Änderungen.

Bei der Aktivierung des Wartungsdiensts wird folgende Meldung zur Protokollausgabe hinzugefügt:

- *N* abgelaufene übergebene Ausführungen in der zugeteilten Zeit entfernt.
- *N* veraltete Ausführungen in der zugeteilten Zeit entfernt.

Weitere Informationen zu den Protokollierungsdiensten finden Sie im *Installations- und Konfigurationshandbuch*.

Batch-Löschung

Das Löschen einer großen Anzahl von Elementen kann langwierig sein, wenn jedes Element gesondert hinzugefügt werden muss. Wenn die Elemente jedoch bestimmte Eigenschaften gemeinsam haben, können Sie das Bereinigungs-Dienstprogramm verwenden, um die Elemente als Gruppe zu identifizieren, auszuwählen und zu löschen. Zur Verwendung dieses Dienstprogramms geben Sie die Kriterien an, die erfüllt sein müssen, damit ein Element ausgewählt und gelöscht wird. Die Auswahlkriterien können auf den folgenden Eigenschaften beruhen:

- Ordner
- MIME-Typ
- Vorliegen eines Labels
- Anzahl der Versionen
- Erstellungsdatum

Beispielsweise können Sie mit dem Bereinigungs-Dienstprogramm bei jeder IBM® SPSS® Statistics-Syntaxdatei in einem bestimmten Ordner alle Versionen bis auf die letzten drei löschen. Oder Sie können alle Versionen ohne Label von IBM® SPSS® Modeler-Streams löschen, die älter sind als ein bestimmtes Datum.

Wenn das automatische Wartungs-Framework aktiviert ist, werden die ausgewählten Elemente für eine anschließende Löschung bei der nächsten verfügbaren Gelegenheit gekennzeichnet. Wenn das Wartungs-Framework deaktiviert ist, werden die Elemente sofort gelöscht.

Das Bereinigungs-Dienstprogramm ist komplett Java-basiert und kann auf jeder unterstützten IBM® SPSS® Collaboration and Deployment Services-Plattform ausgeführt werden. Das Dienstprogramm steht in folgendem Ordner zur Verfügung:

<Repository-Installationspfad>/applications/cleanup

Beachten Sie, dass die Elementlöschung endgültig ist. Gelöschte Elemente können nicht wiederhergestellt werden. Zur Vermeidung unnötiger Risiken sollten Sie die Daten sichern, bevor Sie Dateien mit diesem Dienstprogramm löschen.

Sie können das Bereinigungs-Dienstprogramm über die Befehlszeile ausführen oder Job-Schritte für die automatische, wiederkehrende Verarbeitung erstellen.

Es wird empfohlen, die Repository-Datenbank zu sichern, bevor Dateien mit diesem Dienstprogramm gelöscht werden. Alternativ können Sie mit der Exportfunktion von IBM SPSS Collaboration and Deployment Services eine Sicherungskopie aller Ordner erstellen, die vom Bereinigungs-Dienstprogramm verarbeitet werden.

Ausführen des Bereinigungs-Dienstprogramms

Der Befehl zur Ausführung des Bereinigungs-Dienstprogramms weist folgende Struktur auf:

```
cleanup <Parameter=Wert Parameter=Wert ...>
```

Auf den Befehl `cleanup` folgt eine leerzeichengetrennte Liste mit Parametern und zugehörigen Werten, die den Löschvorgang definieren. Die einzelnen Parameterangaben enthalten den Parameternamen, ein Gleichheitszeichen sowie den Parameterwert. In der Tabelle "Parameter des Bereinigungs-Dienstprogramms" sind die einzelnen Parameter beschrieben.

Tabelle 12-1
Parameter des Bereinigungs-Dienstprogramms

Parameter	Verwenden	Beschreibung
connectionURL	Erforderlich	Die IBM® SPSS® Collaboration and Deployment Services Repository-URL
userid	Erforderlich	Eine gültige native IBM® SPSS® Collaboration and Deployment Services-Benutzer-ID für die Verbindung mit dem Repository-Server. Der Benutzer muss über ausreichende Berechtigungen zum Löschen aller ausgewählten Elemente verfügen. Typischerweise gehört die ID zu einem Administrator.
password	Erforderlich	Das Passwort für den angegebenen Benutzer
resource	Erforderlich	Der Pfad zu einem Repository-Ordner bzw. einer Repository-Datei. Dieser Parameter kann mehrmals angegeben werden.
includeSubFolders	Optional	Ein boolescher Wert, der angibt, ob Unterordner durchsucht werden sollen oder nicht. Die Standardeinstellung ist "falsch".
includeType	Optional	MIME-Typen der aufzunehmenden Objekte. Bei dem Vergleich wird die Groß- und Kleinschreibung nicht berücksichtigt, der Text muss jedoch genau übereinstimmen. Dieser Wert kann mehrmals angegeben werden. Standardmäßig werden alle Typen eingeschlossen.

Parameter	Verwenden	Beschreibung
excludeType	Optional	MIME-Typen der auszuschließenden Objekte. Bei dem Vergleich wird die Groß- und Kleinschreibung nicht berücksichtigt, der Text muss jedoch genau übereinstimmen. Dieser Wert kann mehrmals angegeben werden. Standardmäßig gibt es keine Ausschlüsse.
deleteLabeled	Optional	Ein boolescher Wert, der angibt, ob Versionen mit Labels gelöscht werden sollen oder nicht. Die Standardeinstellung ist “falsch”.
versionsToKeep	Optional	Die Anzahl der aktuellsten Versionen, die beibehalten werden sollen. Die Standardeinstellung lautet 0.
olderThan	Optional	Es werden nur Ressourcen ausgewählt, die vor dem angegebenen Datum erstellt wurden. Damit ein Vergleich möglich ist, werden die Zeitangaben für den Computer, auf dem das Bereinigungs-Dienstprogramm ausgeführt wird, lokalisiert. Standardmäßig gibt es keinen Datumsfilter.
logfile	Optional	Der Pfad zu einer logischen Datei, die zur Protokollierung der Ergebnisse verwendet wird. Standardmäßig gibt es keine Protokolldatei.
testMode	Optional	Ein boolescher Wert, der angibt, ob die ausgewählten Elemente gelöscht werden sollen oder nicht. Der Wert *true* (wahr) führt dazu, dass die Objekte/Versionen ausgewählt werden, ohne tatsächlich gelöscht zu werden. Die Standardeinstellung ist “falsch”.

Das Bereinigungs-Dienstprogramm kann mit folgenden Schritten aufgerufen werden:

1. Vergewissern Sie sich, dass die Umgebungsvariable *Path* (Pfad) Ihren Java-Pfad enthält.
2. Navigieren Sie an einer Eingabeaufforderung zu dem Verzeichnis, das das Bereinigungs-Dienstprogramm enthält.
3. Geben Sie cleanup, gefolgt von der Liste der Parameter und Werte ein, die Ihre Löschaufgabe definieren.
4. Die Aufgabe wird durch Eingabe des Befehls initiiert.

Mit dem folgenden Befehl werden beispielsweise alle Unterordner im Ordner */CleanupData* einbezogen und es werden Versionen ohne Label zum Löschen ausgewählt. Der Parameter testMode verhindert, dass die Versionen tatsächlich gelöscht werden, sodass Sie die Datei *cleanup.log* überprüfen können, um die ausgewählten Versionen zu sehen, die ohne den Parameter testMode gelöscht werden würden.

```
cleanup userid=admin password=pass connectionURL=http://localhost:8080
  testMode=true resource=/CleanupData includeSubFolders=true logfile=cleanup.log
```

Jobs für die Batch-Löschung

Mithilfe eines allgemeinen Job-Schritts können Sie die Batch-Löschung aus einem IBM® SPSS® Collaboration and Deployment Services-Job initiieren. Gehen Sie wie folgt vor, um einen Job-Schritt für die Batch-Löschung in IBM® SPSS® Collaboration and Deployment Services Deployment Manager zu erstellen:

1. Fügen Sie einen allgemeinen Jobschritt zu einem Job hinzu.
2. Klicken Sie auf den Job-Schritt, um die Eigenschaften zu ändern.
3. Geben Sie auf der Registerkarte “Allgemein” einen Namen für den Schritt ein. Geben Sie unter Auszuführender Befehl den vollständigen Pfad zum Bereinigungs-Dienstprogramm für Ihr System ein, gefolgt von Parametern für das Bereinigungs-Dienstprogramm, in dem die Löschaufgabe definiert wird.
4. Wenn die Löschaufgabe den Parameter logfile beinhaltet und das Protokoll im IBM® SPSS® Collaboration and Deployment Services Repository gespeichert werden soll, verwenden Sie die Registerkarte “Ausgabedateien” zur Angabe des Zielspeicherorts für die Datei.
5. Speichern des Jobs.

Der Job kann nach Bedarf manuell ausgeführt werden oder Sie können einen Zeitplan erstellen, mit dem der Job automatisch zu bestimmten Zeiten oder als Reaktion auf Systemereignisse ausgeführt wird. Weitere Informationen zu allgemeinen Jobschritten und zum Planen von Jobs finden Sie in der Deployment Manager-Dokumentation.

Kapitel
13

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.xsl* und *job_failure.xsl*, 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 13-1
Generische Benachrichtigungsmeldung

Weitere Informationen zu Velocity finden Sie in der Dokumentation des Apache Velocity Project (*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 9 auf S. 71. 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 13-1
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	MailSmtpFrom	Die E-Mail-Adresse, die für den Befehl SMTP MAIL verwendet wird. Dadurch wird die Umschlagadresse eingestellt.
mail.smtp.from	Label	MailSmtpFromPersonal	Das Umschlagadress-Label
mail.smtp.localhost	Wert	MailSmtpLocalhost	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	MailSmtpEhlo	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	MailSmtpAuth	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	MailSmtpDsnNotify	Gibt die Umstände an, unter denen der SMTP-Server Benachrichtigungen über den Zustellungsstatus an den Absender der Meldung senden soll. Gültige Werte sind: ■ 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 Ereigniseigenschaften 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 Ereigniseigenschaftswerte 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.

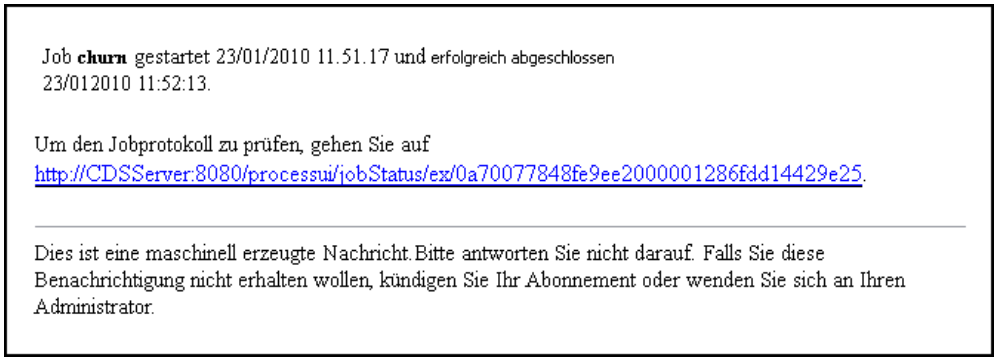
```
<html>
<head>
<meta http-equiv='Content-Type' content='text/html;charset=utf-8'/>
</head>
<body>
<p>Der Job <b>${JobName}</b> wurde am ${JobStart} gestartet und #if($JobSuccess) erfolgreich abgeschlossen #else ist fehlgeschlager

<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 mö
</body>
</html>
```

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

Abbildung 13-2
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.

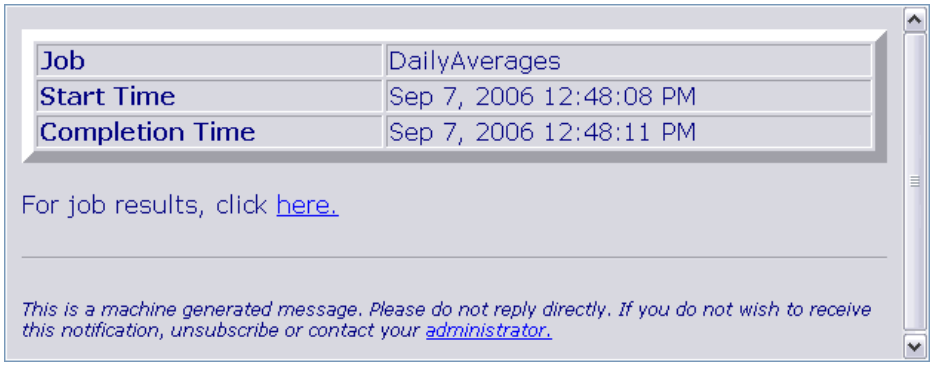
HTML-Benachrichtigungsvorlagen können die Funktionen nutzen, die im Markup erlaubt sind. Zum Beispiel kann die Meldung einen Link auf eine Webseite oder zu einer Job-Ausgabe enthalten.

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 13-3
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 Ereigniseigenschaftsvariablen in das Benachrichtigungsthema einzufügen. Für weitere Informationen siehe Thema Meldungsinhalt auf S. 107.
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. 109.
4. Ändern Sie den Wert, der messageContent zugeordnet ist. Verwenden Sie die $-Notation, um Ereigniseigenschaftsvariablen 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.

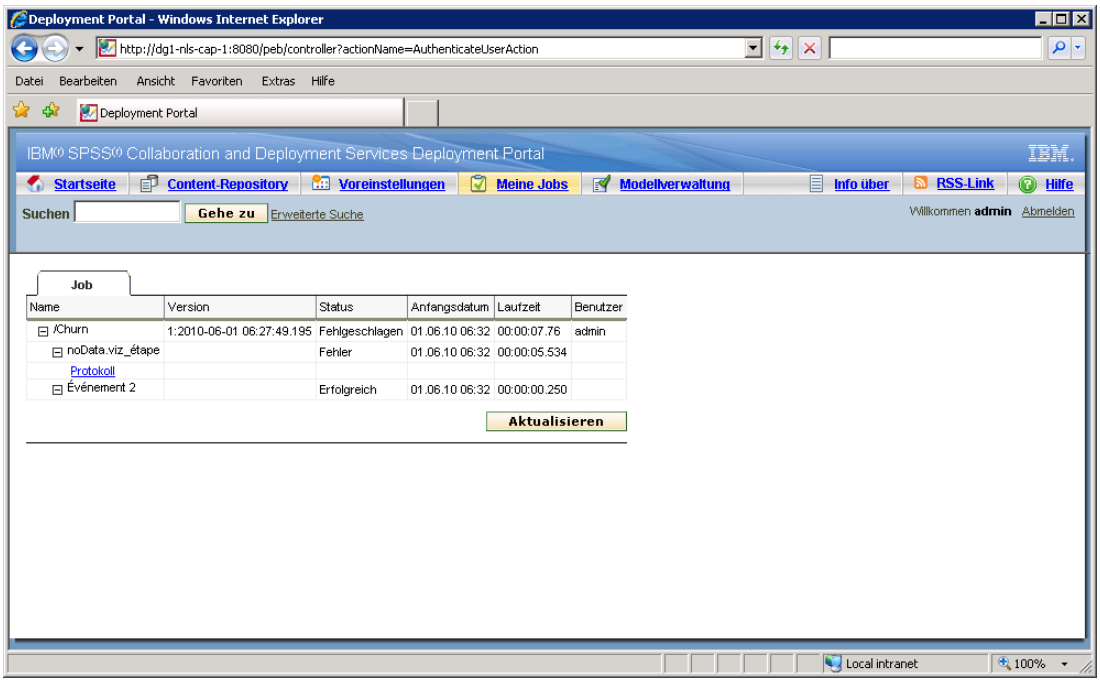
Jobstatus

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 13-4
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*.

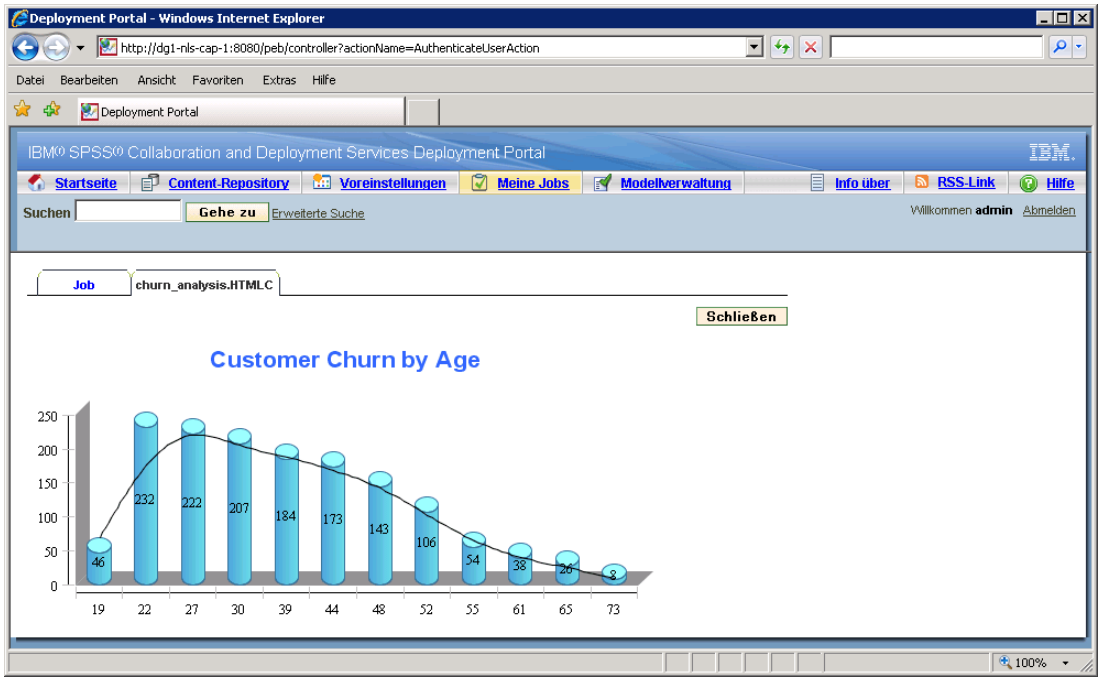
Anfangsdatum. Datum und Uhrzeit des Beginns der Jobschrittverarbeitung.

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 13-5
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. 71

Dedizierter SMTP-Server

Die Leistung des Zustellungskanals, 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. 111. 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 Aktiviäten 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 Bearbeitungmöglichkeiten für die Protokollierungskonfiguration der eingesetzten Komponenten zur Verfügung stellen. Um die SMTP-Protokollierung zu aktivieren, stellen Sie die Konfigurationsoption *SMPT - 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:

[...SmtpDistributor] 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 9 auf S. 71.

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 15.
- Um die Ursache der fehlgeschlagenen Benachrichtigung zu bestimmen, sollten Sie den Debugging-Modus aktivieren. Für weitere Informationen siehe Thema Fehlersuche im Benachrichtigungsdienst auf S. 117.
- *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 15 auf S. 123.

Kapitel
14

JMS-Konfiguration

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 WebLogic. Informationen über das Einrichten von JMS-Providern finden Sie in der Dokumentation des jeweiligen Anbieters.

Die JMS-Einstellungen des Anwendungsservers können geändert werden, um die Limits für Gleichzeitigkeit zu erhöhen, wenn die Leistung von IBM SPSS Collaboration and Deployment Services optimiert werden muss, beispielsweise wenn eine große Anzahl an Jobs gleichzeitig verarbeitet wird. Informationen zur Erhöhung des JMS-Limits für die Gleichzeitigkeit finden Sie im Thema weiter unten. Dieses Kapitel bietet ebenfalls ein Beispiel dafür, wie die Jobverarbeitung auf der Grundlage der Repository-Ereignisse eingerichtet werden kann.

Erhöhen der JMS-Limits für die Gleichzeitigkeit

Wenn aufgrund einer hohen Arbeitsauslastung die Leistungsfähigkeit von IBM® SPSS® Collaboration and Deployment Services optimiert werden muss, beispielsweise weil eine große Anzahl an Jobs gleichzeitig ausgeführt wird, kann es notwendig sein, die JMS-Einstellung des Anwendungsservers zu ändern, um die Limits für die Gleichzeitigkeit zu erhöhen. Im Folgenden werden die allgemeinen Schritte für WebSphere, JBoss und WebLogic beschrieben. Detailliertere Informationen finden Sie in der Dokumentation zum Anwendungsserver.

WebSphere

- Wählen Sie in WebSphere Integrated Solutions Console folgende Optionen aus:
  Ressourcen > JMS > Activation Specifications
- Öffnen Sie *SPSSProcessEventActivationSpec* und erhöhen Sie den Wert von *Maximum concurrent MDB invocations per endpoint* (Maximale gleichzeitige MDB-Aufrufe pro Endpunkt).
- Starten Sie den Server neu.

JBoss

- Ändern Sie *jboss.xml* in *process-ejb.jar* in *process-ejb.ear*, die sich unter *<JBoss-Serververzeichnis>/deploy* befindet, so, dass der Wert des Elements MaximumSize erhöht wird.
- Ändern Sie die globale Einstellung für den JBoss-Server, indem Sie den Wert des Elements MaximumSize unter *<JBoss-Serververzeichnis>/conf/standardjboss.xml* erhöhen.
- Starten Sie den Server neu.

WebLogic

- Verwenden Sie einen WebLogic Work Manager zur Steuerung der Anzahl aktiver Threads.
  - Erstellen Sie einen neuen Work Manager und richten Sie ihn auf den WebLogic-Server aus, der zur Ausführung von IBM SPSS Collaboration and Deployment Services verwendet wird.
  - Aktualisieren Sie den Bereitstellungsdeskriptor, sodass er auf den neuen Work Manager verweist.
  - Ändern Sie *weblogic-ejb-jar.xml* in *process-ejb.jar*, zu finden unter*<Repository-Installationsverzeichnis>/platform/deployables/process-ejb.ear*. Ergänzen Sie folgenden Code:

```
<dispatch-policy>PASWWorkManager</dispatch-policy>
<weblogic-enterprise-bean>
<ejb-name>ProcessEventMDB</ejb-name>
<message-driven-descriptor>
<pool>
<max-beans-in-free-pool>20</max-beans-in-free-pool>
<initial-beans-in-free-pool>1</initial-beans-in-free-pool>
</pool>
<destination-jndi-name>queue/SPSSProcess</destination-jndi-name>
<connection-factory-jndi-name>
ProcessConnectionFactory
</connection-factory-jndi-name>
</message-driven-descriptor>
<dispatch-policy>PASWWorkManager</dispatch-policy>
</weblogic-enterprise-bean>
```

  - Aktualisieren Sie *process-ejb.ear* auf dem Anwendungsserver und passen Sie die zugehörigen Einstellungen in der Administrationskonsole an.

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, löst der Zeitplan den Job aus. Weitere Informationen finden Sie im *Deployment Manager 5-Benutzerhandbuch*.

Kapitel
15

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 Ergebnisset 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-Ausführungsereignisse

- 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—Grupppe 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—Änderungsereignis für Benachrichtigungs- oder Abonnementeinstellungen (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, eineIBM® 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.

ATTRIBUTECATEGORICALVALUE. 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 FileOuput-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-Servicedaten 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_METRIC 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
```

Erfolglose 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-Ressources (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'
```

Anhang

A

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="lalger" 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 A-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 encrypted-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 *nicht* 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 encrypted-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>
```

Anhang

B

Hinweise

Diese Informationen wurden für weltweit angebotene Produkte und Dienstleistungen erarbeitet.

IBM bietet die in diesem Dokument behandelten Produkte, Dienstleistungen oder Merkmale möglicherweise nicht in anderen Ländern an. Informationen zu den in derzeit in Ihrem Land erhältlichen Produkten und Dienstleistungen erhalten Sie bei Ihrem zuständigen IBM-Mitarbeiter vor Ort. Mit etwaigen Verweisen auf Produkte, Programme oder Dienste von IBM soll nicht behauptet oder impliziert werden, dass nur das betreffende Produkt oder Programm bzw. der betreffende Dienst von IBM verwendet werden kann. Stattdessen können alle funktional gleichwertigen Produkte, Programme oder Dienste verwendet werden, die keine geistigen Eigentumsrechte von IBM verletzen. Es obliegt jedoch der Verantwortung des Benutzers, die Funktionsweise von Produkten, Programmen oder Diensten von Drittanbietern zu bewerten und zu überprüfen.

IBM verfügt möglicherweise über Patente oder hat Patentanträge gestellt, die sich auf in diesem Dokument beschriebene Inhalte beziehen. Durch die Bereitstellung dieses Dokuments werden Ihnen keinerlei Lizenzen an diesen Patenten gewährt. Lizenzanfragen können schriftlich an folgende Adresse gesendet werden:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, U.S.A.

Bei Lizenzanfragen in Bezug auf DBCS-Daten (Double-Byte Character Set) wenden Sie sich an die für geistiges Eigentum zuständige Abteilung von IBM in Ihrem Land. Schriftliche Anfragen können Sie auch an folgende Adresse senden:

Intellectual Property Licensing, Legal and Intellectual Property Law, IBM Japan Ltd., 1623-14, Shimotsuruma, Yamato-shi, Kanagawa 242-8502 Japan.

Der folgende Absatz gilt nicht für Großbritannien oder andere Länder, in denen derartige Bestimmungen nicht mit dem dort geltenden Recht vereinbar sind. INTERNATIONAL BUSINESS MACHINES ÜBERNIMMT FÜR DIE VORLIEGENDE DOKUMENTATION KEINERLEI GEWÄHRLEISTUNG IRGENDWELCHER ART, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, EINSCHLIESSLICH (JEDOCH NICHT DARAUF BEGRENZT) DER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN IN BEZUG AUF DIE NICHTVERLETZUNG VON RECHTEN DRITTER, AUF HANDELSÜBLICHKEIT ODER DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. Einige Staaten lassen bei bestimmten Transaktionen keine Ausschlussklauseln ausdrücklicher oder stillschweigender Gewährleistungen zu, sodass diese Erklärung möglicherweise nicht auf Sie zutrifft.

Diese Informationen können technische Ungenauigkeiten oder typografische Fehler enthalten. An den hierin enthaltenen Informationen werden in regelmäßigen Abständen Änderungen vorgenommen, die in spätere Ausgaben der Publikation eingearbeitet werden. IBM kann jederzeit ohne Vorankündigung Verbesserungen und/oder Veränderungen an den in dieser Publikation beschriebenen Produkten und/oder Programmen vornehmen.

Alle in diesen Ausführungen enthaltenen Verweise auf Websites, die nicht zu IBM gehören, dienen lediglich der Information. Die Nennung bedeutet nicht, dass IBM den Inhalt dieser Websites unterstützt. Das Material auf diesen Websites ist kein Bestandteil des Materials für dieses IBM-Produkt. Sie verwenden diese Websites auf eigene Gefahr.

IBM ist berechtigt, die von Ihnen bereitgestellten Informationen in jeglicher Form zu verwenden bzw. weiterzugeben, die dem Unternehmen geeignet erscheint, ohne dass ihm daraus Verbindlichkeiten Ihnen gegenüber entstehen.

Lizenznehmer dieses Programms, die Informationen dazu benötigen, wie (i) der Austausch von Informationen zwischen unabhängig erstellten Programmen und anderen Programmen und (ii) die gegenseitige Verwendung dieser ausgetauschten Informationen ermöglicht wird, wenden sich an:

IBM Software Group, Attention: Licensing, 233 S. Wacker Dr., Chicago, IL 60606, USA.

Diese Informationen sind je nach den entsprechenden Geschäftsbedingungen und in manchen Fällen gegen Zahlung einer Gebühr erhältlich.

Das in diesem Dokument beschriebene lizenzierte Programm und sämtliche dafür verfügbaren lizenzierten Materialien werden von IBM gemäß dem IBM-Kundenvertrag, den Internationalen Nutzungsbedingungen für Programmpakete der IBM oder einer anderen zwischen uns getroffenen Vereinbarung bereitgestellt.

Alle in diesem Dokument enthaltenen Leistungsdaten wurden in einer kontrollierten Umgebung ermittelt. Daher können die unter anderen Betriebsumgebungen erzielten Ergebnisse erheblich abweichen. Einige Messungen wurden möglicherweise an Systemen im Entwicklungsstadium vorgenommen und es besteht keine Garantie, dass spätere allgemein verfügbare Systeme dieselben Messwerte aufweisen. Außerdem wurden einige Messwerte möglicherweise mittels Extrapolation geschätzt. Die tatsächlichen Ergebnisse können abweichen. Die Benutzer dieses Dokuments sollten die entsprechenden Daten für ihre jeweilige Umgebung überprüfen.

Informationen zu Nicht-IBM-Produkten stammen von den Herstellern dieser Produkte, ihren veröffentlichten Verlautbarungen oder aus anderen öffentlich verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher die Richtigkeit der Angaben zu Leistung und Kompatibilität oder anderer Behauptungen in Bezug auf Nicht-IBM-Produkte nicht bestätigen. Fragen zu den Fähigkeiten von Nicht-IBM-Produkten sind an die Hersteller dieser Produkte zu richten.

Alle Aussagen in Bezug auf die zukünftige Ausrichtung oder die zukünftigen Vorhaben von IBM können ohne Vorankündigung geändert oder widerrufen werden und stellen lediglich Zielsetzungen dar.

Diese Informationen enthalten Beispiele für Daten und Berichte, die in alltäglichen Betriebsabläufen verwendet werden. Um sie möglichst umfassend darzulegen, enthalten die Beispiele Namen von Einzelpersonen, Unternehmen, Marken und Produkten. Alle diese Namen sind frei erfunden und jegliche Ähnlichkeit mit den von einem tatsächlichen Handelsunternehmen verwendeten Namen und Adressen ist rein zufällig.

Bei der Anzeige dieser digitalen Informationsversion sind die Fotografien und Farbillustrationen möglicherweise nicht sichtbar.

Trademarks

IBM, das IBM-Logo, ibm.com und SPSS sind Marken von IBM Corporation, die in vielen Ländern weltweit eingetragen sind. Eine aktuelle Liste der IBM-Marken finden Sie im Internet unter *http://www.ibm.com/legal/copytrade.shtml*.

Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind eingetragene Marken oder Marken von Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Intel, das Intel-Logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium und Pentium sind Marken oder eingetragene Marken von Intel Corporation oder seinen Tochtergesellschaften in den USA und anderen Ländern.

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

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken von Microsoft Corporation in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Java und alle Java-basierten Marken und Logos sind Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

Weitere Produkt- oder Servicenamen können Marken von IBM oder anderen Unternehmen sein.

Index