IBM SPSS Collaboration and Deployment Services
Version 8 Release 2

Administratorhandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 111 gelesen werden.

Produktinformation

Diese Ausgabe bezieht sich auf Version 8, Release 2, Modifikation 1 von IBM SPSS Collaboration and Deployment Services und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

Inhaltsverzeichnis

Kapitel 1. Übersicht

IBM SPSS Collaboration and Deployment Services

IBM® SPSS Collaboration and Deployment Services ist eine Anwendung auf Unternehmensebene, die die weit verbreitete Verwendung von Vorhersageanalytiken gestattet.

IBM SPSS Collaboration and Deployment Services bietet Benutzern eine zentrale, sichere und überprüfbare Speicherung von Analyseassets sowie erweiterte Funktionen für die Verwaltung und Steuerung von Analyseprozessen zur Vorhersage sowie hoch entwickelte Mechanismen zur Bereitstellung der Ergebnisse der analytischen Verarbeitung. Zu den Vorteilen von IBM SPSS Collaboration and Deployment Services zählen:

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

IBM SPSS Collaboration and Deployment Services ermöglicht Ihnen die sichere Verwaltung verschiedener Analyseassets und fördert die Zusammenarbeit zwischen den Entwicklern und den Benutzern. Darüber hinaus stellen die Bereitstellungsfunktionen sicher, dass die verantwortlichen Personen die benötigten Informationen erhalten, um rechtzeitig die entsprechenden Aktionen ausführen zu können.

Zusammenarbeit

Zusammenarbeit bezieht sich auf die Fähigkeit, Analyseassets effizient gemeinsam zu nutzen und wiederholt zu verwenden. Sie ist der Schlüssel zur Entwicklung und Implementierung von Analysen in einem Unternehmen.

Analysten brauchen einen Ort, an dem sie Dateien platzieren können, die anderen Analysten oder Fachanwendern zur Verfügung stehen sollen. An diesem Ort muss eine Versionssteuerung 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. In IBM SPSS Collaboration and Deployment Services Repository gespeicherte Dateien sind für alle Benutzer im gesamten Unternehmen verfügbar, sofern diese über die entsprechenden Zugriffsberechtigungen verfügen. Zum Auffinden der gewünschten Informationen bietet das Repository eine Suchfunktion.

Analysten können die Dateien im Repository mithilfe von Clientanwendungen bearbeiten, die 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 Analyst kann eine Version einer in Entwicklung befindlichen Datei speichern, diese Version zu einem späteren Zeitpunkt abrufen und mit der Bearbeitung der Datei fortfahren, bis diese abgeschlossen ist und die Datei in einen Produktionsprozess verlagert werden kann. Diese Dateien können benutzerdefinierte Schnittstellen enthalten, die Analyseprozesse ausführen und Fachanwendern die Möglichkeit geben, die Vorteile aus der Arbeit eines Analysten zu nutzen.

Der Einsatz des Repositorys schützt das Unternehmen, indem es einen zentralen Speicherort für Analyseassets bietet, der sich bequem sichern und wiederherstellen lässt. Zudem steuern Berechtigungen auf Benutzer-, Datei- und Versionsebene den Zugriff auf die individuellen Bereiche. Versionssteuerung und Ob-

jektversionsbeschriftungen stellen sicher, dass die korrekten Versionen der Daten in Produktionsprozessen verwendet werden. Schließlich bieten die Protokollierungsfunktionen die Möglichkeit, Datei- und Systemänderungen zu verfolgen.

Bereitstellung

Damit alle Vorteile der Vorhersageanalyse nutzbar sind, müssen die Analyseassets Informationen 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 die Verarbeitung von **Jobs** eingeschlossen werden. Jobs legen eine Ausführungssequenz für analytische Artefakte fest und können mithilfe von IBM SPSS Deployment Manager erstellt werden. Die Ausführungsergebnisse können im Repository oder auf einem Dateisystem gespeichert oder an angegebene Empfänger übergeben werden. Auf die im Repository gespeicherten Ergebnisse kann jeder Benutzer mit den entsprechenden Berechtigungen über die Benutzerschnittstelle von IBM SPSS Collaboration and Deployment Services Deployment Portal zugreifen. Die Jobs können nach einem definierten Zeitplan oder als Reaktion auf Systemereignisse ausgelöst werden.

Ferner ist es mit dem Scoring-Service von IBM SPSS Collaboration and Deployment Services möglich, Analyseergebnisse beim Kontakt mit einem Kunden aus bereitgestellten Modellen in Echtzeit zu übermitteln. 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 Single Sign-on reduzieren sich manuelle Eingaben von Berechtigungsnachweisen 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 einer einzigen, zentralen Instanz von IBM SPSS Collaboration and Deployment Services Repository, die eine Vielzahl von Clients mithilfe von Ausführungsservern zur Verarbeitung von Analyseassets bedient.

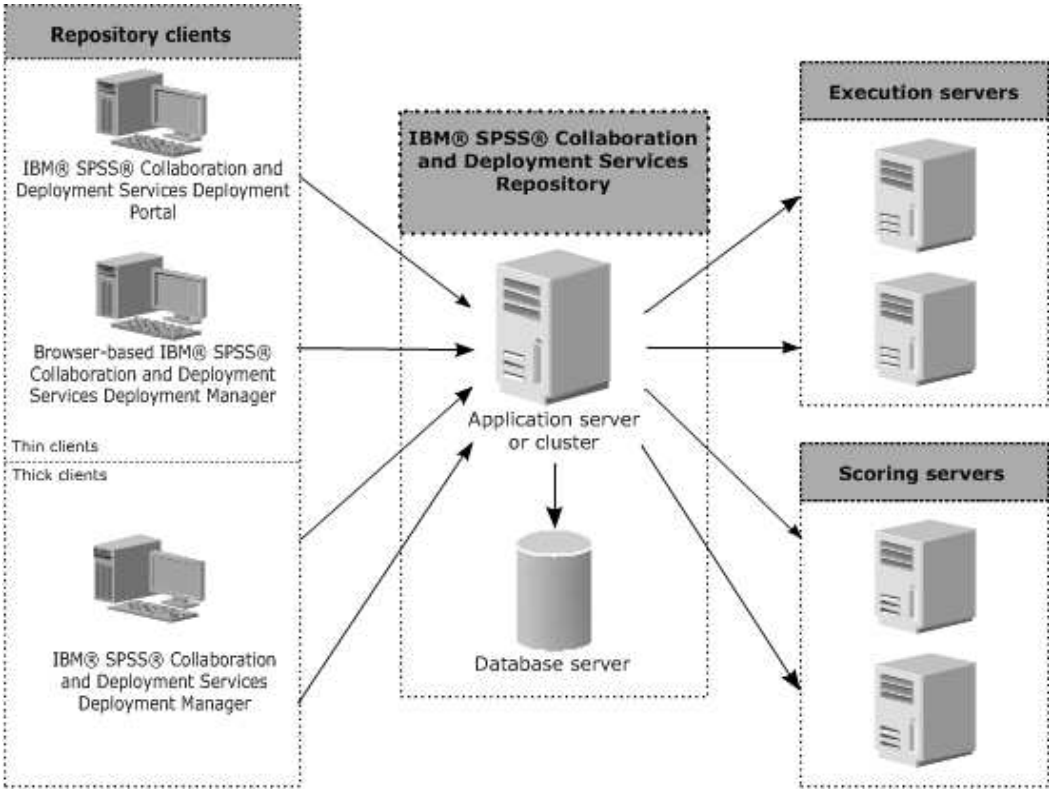

Abbildung 1. Architektur von IBM SPSS Collaboration and Deployment Services

IBM SPSS Collaboration and Deployment Services besteht aus den folgenden Komponenten:

- IBM SPSS Collaboration and Deployment Services Repository für analytische Artefakte
- IBM SPSS Deployment Manager
- IBM SPSS Collaboration and Deployment Services Deployment Portal
- Browserbasierte Instanz von IBM SPSS Deployment Manager

IBM SPSS Collaboration and Deployment Services Repository

Das Repository ist ein zentraler Ort, an dem Analyseassets, wie Modelle und Daten, gespeichert werden können. Das Repository erfordert die Installation einer relationalen Datenbank, wie IBM Db2, Microsoft SQL Server oder Oracle.

Das Repository umfasst Funktionen für:

- Sicherheit
- Versionssteuerung
- Suchen
- Auditing

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

IBM SPSS Deployment Manager

IBM SPSS Deployment Manager ist eine Clientanwendung 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.

Mit der Clientanwendung kann ein Benutzer die folgenden Aufgaben ausführen:

- Anzeigen aller vorhandenen Dateien im System, einschließlich -Berichten, SAS-Syntaxdateien, und Datendateien
- Importieren von Dateien in das Repository
- Planung wiederholt auszuführender Jobs mithilfe eines bestimmten Wiederholungsmusters, z. B. vierteljährlich oder stündlich
- Ändern vorhandener Jobeigenschaften
- Bestimmen des Status eines Jobs
- Angeben von E-Mail-Benachrichtigungen zum Jobstatus

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

- Benutzer verwalten
- Sicherheitsprovider konfigurieren
- Rollen und Aktionen zuweisen

Browserbasierte Instanz von IBM SPSS Deployment Manager

Die browserbasierte Instanz von IBM SPSS Deployment Manager ist eine Thin-Client-Benutzerschnittstelle für die Ausführung von Einrichtungs- und Systemmanagementaufgaben wie:

- Festlegen von Optionen zur Systemkonfiguration
- Konfigurieren von Sicherheitsprovidern
- Verwalten von MIME-Typen

Benutzer ohne Verwaltungsaufgaben können all diese Aufgaben ausführen, wenn die entsprechenden Aktionen ihren Anmeldeberechtigungsnachweisen zugeordnet sind. Die Aktionen werden von einem Administrator zugewiesen.

In der Regel greifen Sie über die folgende URL auf die browserbasierte Instanz von IBM SPSS Deployment Manager zu:

```
http://<IP-Adresse_des_Hosts>:<Port>/security/login
```

Anmerkung: Eine IPv6-Adresse muss in eckige Klammern eingeschlossen werden, z. B. `[3ffe:2a00:100:7031::1]`.

Wenn Ihre Umgebung für die Verwendung eines benutzerdefinierten Kontextpfads für Serververbindungen konfiguriert ist, schließen Sie diesen Pfad in die URL ein.

```
http://<IP-Adresse_des_Hosts>:<Port>/<Kontextpfad>/security/login
```

IBM SPSS Collaboration and Deployment Services Deployment Portal

IBM SPSS Collaboration and Deployment Services Deployment Portal ist eine Thin-Client-Benutzerschnittstelle für den Zugriff auf das Repository. Im Gegensatz zur browserbasierten Instanz von IBM SPSS Deployment Manager, die für Administratoren gedacht ist, ist IBM SPSS Collaboration and Deployment Services 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 Inhalt
- Ausführen von Jobs und Berichten
- Generieren von Scores anhand von im Repository gespeicherten Modellen
- Durchsuchen des Repository-Inhalts
- Anzeigen von Inhaltseigenschaften
- Zugriff auf individuelle Benutzervorgaben wie E-Mail-Adresse und Kennwort, auf allgemeine Optionen, Abonnements und Optionen für Ausgabedateiformate

In der Regel greifen Sie über die folgende URL auf die Homepage zu:
`http://<IP-Adresse_des_Hosts>:<Port>/peb`

Anmerkung: Eine IPv6-Adresse muss in eckige Klammern eingeschlossen werden, z. B. `[3ffe:2a00:100:7031::1]`.

Wenn Ihre Umgebung für die Verwendung eines benutzerdefinierten Kontextpfads für Serververbindungen konfiguriert ist, schließen Sie diesen Pfad in die URL ein.
`http://<IP-Adresse_des_Hosts>:<Port>/<Kontextpfad>/peb`

Ausführungsserver

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

Zu den aktuellen von IBM SPSS Collaboration and Deployment Services unterstützten Ausführungsservern zählen die folgenden:

- **Fernverarbeitung**. Ein Ausführungsserver für Fernverarbeitungen ermöglicht den Start und die Überwachung von Prozessen auf fernen Servern. Nach Abschluss des Prozesses wird eine Nachricht über den Erfolg bzw. Misserfolg ausgegeben. Auf allen Rechnern, die als Fernverarbeitungsserver fungieren, muss die zur Kommunikation mit dem Repository benötigte Infrastruktur installiert sein.

  Anmerkung: IBM SPSS Collaboration and Deployment Services Remote Process Server hat eine Standard-Thread-Pool-Kerngröße von 16. Dadurch können 16 gleichzeitige Jobs auf einem einzigen Fernverarbeitungsserver ausgeführt werden. Wird die Anzahl 16 überschritten, muss jeder weitere gleichzeitige Job in der Warteschlange warten, bis der verfügbare Thread-Pool über freie Ressourcen verfügt. Wenn Sie die Thread-Pool-Kerngröße von IBM SPSS Collaboration and Deployment Services Remote Process Server manuell konfigurieren wollen, fügen Sie dem Startscript des Fernverarbeitungsservers die folgende JVM-Option (mit einem benutzerdefinierten Wert) hinzu:
  `prms.thread.pool.coresize=<benutzerdefinierter Wert>`

  Weitere Informationen zum Startscript finden Sie im Abschnitt "Starten und Stoppen von Remote Process Server" im Handbuch zu IBM SPSS Collaboration and Deployment Services Remote Process Server.

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 sogenannter Scoring Server, verfügbar.

Scoring Server verbessert die Bereitstellungsflexibilität in mehreren wichtigen Bereichen:

- Die Scoring-Leistung kann unabhängig von anderen Services skaliert werden.
- Scoring Server können unabhängig voneinander konfiguriert werden, um Computerressourcen einer oder mehreren Scoring-Konfiguration(en) von IBM SPSS Collaboration and Deployment Services zuzuteilen.
- Betriebssystem und Prozessorarchitektur des Scoring Servers brauchen nicht mit 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.

IBM Analytical Decision Management

IBM SPSS Collaboration and Deployment Services ist eine Voraussetzung für die Installation von IBM Analytical Decision Management, einer Anwendungssuite zur Integration von Vorhersageanalysen in die betrieblichen Entscheidungsfindungsprozesse. IBM Analytical Decision Management verwendet schnelles Scoring, Masterdatenmanagement 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.

Lizenzüberwachung

Bei der Verwendung von IBM SPSS Collaboration and Deployment Services wird die Lizenznutzung überwacht und in regelmäßigen Intervallen protokolliert. Es werden die Lizenzmetriken *AUTHORIZED_USER* und *CONCURRENT_USER* protokolliert und der Typ der protokollierten Metrik ist von Ihrem Lizenztyp für IBM SPSS Collaboration and Deployment Services abhängig.

Die erstellten Protokolldateien können vom Produkt IBM License Metric Tool verarbeitet werden, über das Sie Lizenznutzungsberichte generieren können.

Die Lizenzprotokolldateien werden in demselben Verzeichnis erstellt, in dem directory where IBM SPSS Collaboration and Deployment Services-Protokolldateien aufgezeichnet werden (standardmäßig `<Benutzerprofil>\AppData\Roaming\SPSSInc\Deployment Manager`).

Kapitel 2. Neuerungen in dieser Version

Neuerungen für Administratoren

IBM SPSS Collaboration and Deployment Services 8.2.1 stellt neue Funktionen bereit, die die Bereitstellung von Vorhersageanalysen erleichtern und Ihnen helfen, die Kosten besser in den Griff zu bekommen.

Unterstützung von IPv6-Multicastadressen

Sie können jetzt über eine Multicastadresse des Typs IPv6 auf den Server mit IBM SPSS Collaboration and Deployment Services Repository verweisen.

Veraltete Features

Wenn Sie von einem früheren Release von IBM SPSS Collaboration and Deployment Services migrieren, müssen Sie beachten, dass viele Features seit der letzten Version veraltet sind und nicht mehr verwendet werden.

Wenn ein Feature veraltet ist, entfernt IBM Corp. dieses Feature möglicherweise in einem nachfolgenden Release des Produkts. Zukünftige Investitionen werden sich auf die unter der empfohlenen Migrationsaktion aufgelistete strategische Funktion konzentrieren. In der Regel wird ein Feature nur dann nicht mehr verwendet, wenn es eine funktional entsprechende Alternative gibt.

In diesem Release wurden keine Features nicht weiter unterstützt. Für Referenzzwecke enthält die folgende Tabelle Features, die in neueren Vorgängerversionen des Produkts nicht weiter unterstützt wurden. Sofern möglich, ist in der Tabelle auch die empfohlene Migrationsaktion angegeben.

Tabelle 1. Veraltete Features aus Vorgängerversionen

Einstellung der Unterstützung	Empfohlene Migrationsaktion
Sicherheitsprovider: Active Directory mit lokaler Übersteuerung, wodurch erweiterte Gruppen und berechtigte Benutzer unterstützt werden	Active Directory-Standardsicherheitsprovider mit gegebenenfalls hinzugefügten erforderlichen Gruppen verwenden
IBM SPSS Collaboration and Deployment Services Enterprise View	Analysedatenansicht verwenden
IBM SPSS Collaboration and Deployment Services Enterprise View Driver	Analysedatenansicht verwenden
Szenariodateien	Szenariodateien (`.scn`) werden nicht weiter unterstützt. Enterprise View-Quellenknoten können in Deployment Manager nicht geändert werden. Alte Szenariodateien können im IBM SPSS Modeler-Client geändert und als Datenstromdateien erneut gespeichert werden. Auch Scoring-Konfigurationen, die eine Szenariodatei verwendet haben, müssen gelöscht und basierend auf einer Datenstromdatei erneut erstellt werden.
Webinstallation für IBM SPSS Deployment Manager	Standalone-Installationsprogramm verwenden
BIRT Report Designer for IBM SPSS	Keine
Viewer von BIRT Report Designer for IBM SPSS	Keine
IBM SPSS Collaboration and Deployment Services Portlet	IBM SPSS Collaboration and Deployment Services Deployment Portal direkt oder die Web-Service-APIs verwenden

Tabelle 1. Veraltete Features aus Vorgängerversionen (Forts.)

Einstellung der Unterstützung	**Empfohlene Migrationsaktion**
IBM SPSS Collaboration and Deployment Services Web Part	IBM SPSS Collaboration and Deployment Services Deployment Portal direkt oder die Web-Service-APIs verwenden
API von Scoring-Service Version 1	API von Scoring-Service Version 2
Zeitplanungsservice	Keine
Berichterstellungsservice	Keine
Operation `login` des Authentifizierungsservice	Operation `doLogin` des Authentifizierungsservice
Operation `search` des Suchservice	Operation `search2.5` des Suchservice
JAR-Datei für SPSS AXIS/Castor-Web-Service-Client	Mit Java Runtime Environment, der integrierten Entwicklungsumgebung (IDE) oder Eclipse Web Tools Platform (WTP) bereitgestellte Tools verwenden
API-Funktion `clemrtl_setLogFile()`	Keine

Kapitel 3. Erste Schritte

Nach der erfolgreichen Installation von 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 Kennwörtern und Navigieren in der Schnittstelle
- Hinzufügen oder Ändern von IBM SPSS Modeler-Unterstützung

Starten des Repository-Servers

Der Repository-Server kann an einer Konsole oder im Hintergrund ausgeführt werden.

Die Ausführung an einer Konsole ermöglicht die Anzeige von Verarbeitungsnachrichten und kann nützlich für die Diagnose von unvorhergesehenem Verhalten sein. Jedoch wird der Repository-Server in der Regel im Hintergrund ausgeführt und verarbeitet Anforderungen von Clients wie z. B. IBM SPSS Modeler oder IBM SPSS 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 die Ausführung an einer Konsole auf einer UNIX-Plattform der Ausführung in einer Shell und die Ausführung im Hintergrund entspricht der Ausführung als Dämon.

Wichtig: Zur Vermeidung von Berechtigungskonflikten muss der Repository-Server immer mit denselben Berechtigungsnachweisen gestartet werden, vorzugsweise durch einen Benutzer mit `sudo`-Berechtigungen (UNIX) oder mit Administratorrechten (Windows).

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

WebSphere

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

WebSphere Liberty-Standalone-Server

Standardmäßig verwendet das enthaltene Liberty-Profil 9080 für den HTTP-Endpunkt und 9443 für den HTTPS-Endpunkt. Wenn Sie diese Portnummern ändern wollen, aktualisieren Sie die Datei `server.xml` im folgenden Verzeichnis:

```
<Repository-Installationsverzeichnis>/wlp/usr/servers/cdsServer
```

Wenn Sie die Standardportnummern verwenden, stellen Sie vor dem Starten des Servers sicher, dass die Portnummer nicht bereits von anderen Anwendungen verwendet wird. Verwenden Sie folgende Scripts für die Repository-Installation:

```
<Repository-Installationsverzeichnis>/bin/startserver.bat
<Repository-Installationsverzeichnis>/bin/startserver.sh
```

Während des WebSphere Liberty-Anwendungprozesses wird zuerst das Liberty-Profil gestartet und anschließend die Anwendung bereitgestellt. Den Repository-Server-Status können Sie in der Datei `cds.log` in `<Repository-Installationsverzeichnis>/wlp/usr/servers/cdsServer/` prüfen.

WebSphere Liberty-Cluster

Stellen Sie die zugehörigen Konfigurationsdateien bereit, bevor Sie den Repository-Server starten, der für Ihren WebSphere Liberty-Cluster bereitgestellt wurde. Diese Dateien sind in Liberty für Verbundmember im Cluster erforderlich und sie umfassen die Konfigurationsdateien in `server.xml` in jedem Verbundmember. Führen Sie vor der Bereitstellung der Konfigurationsdateien folgende Schritte aus:

1. Konfigurieren Sie das Installationsverzeichnis, das gemeinsam genutzt werden soll, und stellen Sie sicher, dass es für alle Member des Clusters zugänglich ist.
2. Stellen Sie sicher, dass `{wlp.usr.dir}` und `{server.config.dir}` für jedes Verbundmember im Cluster hinzugefügt werden, damit Whitelist-Einträge geschrieben werden. Dies muss in der Datei `server.xml` für den Verbundcontroller erfolgen. In der Dokumentation zu WebSphere Liberty finden Sie ausführliche Informationen hierzu.
3. Vergewissern Sie sich für WebSphere Liberty unter Windows, dass RXA ordnungsgemäß eingerichtet ist.
4. Starten Sie den Verbundcontroller und alle Verbundmember im Cluster.

Verwenden Sie folgende Scripts für die Repository-Server-Installation:

```
<Repository-Installationsverzeichnis>/bin/deployUtility.bat -cads_home ${CDS_HOME}
<Repository-Installationsverzeichnis>/bin/deployUtility.sh -cads_home ${CDS_HOME}
```

Dabei steht `${CDS_HOME}` für den gemeinsam genutzten Speicherort der IBM SPSS Collaboration and Deployment Services-Systemdateien. Für alle Verbundmember muss der Zugriff auf diesen Speicherort über die Dateifreigabe unter Windows oder NFS unter Linux/UNIX möglich sein.

Starten Sie danach alle Verbundmember im Cluster erneut, damit die neu bereitgestellten Konfigurationsdateien geladen werden.

JBoss

Verwenden Sie folgende Scripts für die Repository-Server-Installation:

```
<Repository-Installationsverzeichnis>/bin/startserver.bat
<Repository-Installationsverzeichnis>/bin/startserver.sh
```

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

Verwenden der browserbasierten Instanz von IBM SPSS Deployment Manager

Die Anmeldungsseite ist Ihr Gateway zum System.

So melden Sie sich an:

1. Navigieren Sie in einem Browser zur Anmeldeseite. Die URL lautet normalerweise wie folgt:
   ```
   http://<IP-Adresse_des_Hosts>:<Port>/security/login
   ```

   Die Verwendung von *localhost* anstelle der IP-Adresse kann bei einigen Anwendungsservern fehlschlagen. Die Verwendung der IP-Adresse wird für alle Fälle empfohlen.

Anmerkung: Eine IPv6-Adresse muss in eckige Klammern eingeschlossen werden, z. B. `[3ffe:2a00:100:7031::1]`.

Wenn Ihre Umgebung für die Verwendung eines benutzerdefinierten Kontextpfads für Serververbindungen konfiguriert ist, schließen Sie diesen Pfad in die URL ein.

```
http://<IP-Adresse_des_Hosts>:<Port>/<Kontextpfad>/security/login
```

2. Geben Sie in das Feld "Anmeldenamen" Ihre Benutzer-ID ein.
3. Geben Sie in das Feld "Kennwort" Ihr Kennwort ein.
4. Klicken Sie auf **Anmelden**.

Wichtig: Für eine erfolgreiche Anmeldung muss Ihr Browser Sitzungscookies zulassen.

Weitere Optionen

Auf der Anmeldeseite haben Sie auch die Möglichkeit, Ihr Kennwort zu ändern. Weitere Informationen finden Sie in „Ändern von Kennwörtern".

Wichtig: Single Sign-on ist für browserbasierte Instanzen von IBM SPSS Deployment Manager nicht gestattet.

Ändern von Kennwörtern

So ändern Sie Ihr Kennwort:

Klicken Sie auf der Anmeldeseite auf **Kennwort ändern?** Das Dialogfeld "Kennwort ändern" wird geöffnet.

1. Geben Sie in das Feld "Anmeldenamen" Ihren Anmeldenamen ein.
2. Geben Sie in das Feld "Aktuelles Kennwort" Ihr aktuelles Kennwort ein.
3. Geben Sie in das Feld "Neues Kennwort" Ihr neues Kennwort ein.
4. Wiederholen Sie in das Feld "Neues Kennwort bestätigen" Ihr neues Kennwort.
5. Klicken Sie auf **Neues Kennwort speichern**. Im Abschnitt "Nachrichten" wird der folgende Text angezeigt:

   ```
   Kennwort aktualisiert
   ```

6. Klicken Sie auf **Zur Anmeldung zurückkehren**. Die Anmeldungsseite wird geöffnet. Melden Sie sich mit Ihrem neuen Kennwort beim System an. Weitere Informationen finden Sie im Thema „Verwenden der browserbasierten Instanz von IBM SPSS Deployment Manager" auf Seite 10.

Navigation durch die browserbasierte Instanz von IBM SPSS Deployment Manager

Die browserbasierte Instanz von IBM SPSS Deployment Manager beruht primär auf der Navigation über Registerkarten.

Im Allgemeinen sind Komponenten des Systems von allgemein bis spezifisch gegliedert. Im Navigationsfenster können Sie beliebige der folgenden Kategorien auswählen:

- **Konfiguration**
- **MIME-Typen**
- **Repository-Index**
- **Sicherheitsprovider**
- **Abmelden**
- **Info über**
- **Administratorhandbuch**
- **Hilfe**

Mit jedem dieser Elemente ist mindestens ein Abschnitt 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 Dateitypsymbole** 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 übergeben. 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

Auf die Informationen zur Installation von IBM SPSS Collaboration and Deployment Services können Sie über die Seite "Info über" zugreifen.

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.

So zeigen Sie detaillierte Informationen für installierte Pakete an:

- Klicken Sie auf **Details anzeigen**.

So laden Sie Versions- und Systeminformationen in Form einer Textdatei herunter:

- Klicken Sie auf **Version und Systemdaten herunterladen**.

So laden Sie Textdateien mit Systeminformationen und dem Anwendungsserverprotokoll herunter:

- Klicken Sie auf **Version, Systemdaten und Protokolle in einer ZIP-Datei herunterladen**. Die Dateien werden als komprimiertes Archiv heruntergeladen.

IBM SPSS Deployment Manager verwenden

Verwaltungsaufgaben können sowohl mit IBM SPSS Deployment Manager als auch mit der browserbasierten Instanz von IBM SPSS Deployment Manager ausgeführt werden. Ein Administrator kann Folgendes ausführen:

- Konfigurieren und Aktivieren von Sicherheitsprovidern
- Erstellen von Benutzer und Gruppen für den Zugriff auf das System
- Definieren von Rollen zur Steuerung des Zugriffs auf Systemfunktionen

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

Erste Schritte

Verwaltete Server

Die Serveradministration in IBM SPSS Deployment Manager umfasst Folgendes:

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

Wählen Sie die folgenden Befehle aus den Menüs aus:

Extras > **Serveradministration**

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

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 neuen verwalteten Servers zum System besteht in der Definition des Serversnamens und -typs.

Name. Eine Beschriftung, mit deren Hilfe der vorherige Server auf der Registerkarte "Serveradministration" 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)
- Et-Zeichen (&)
- Kleiner-als- (<) und Größer-als-Zeichen (>)
- Schrägstrich (/)
- Punkte
- Kommas
- Semikolons

Typ. Typ des Servers, der hinzugefügt wird. Die Liste der möglichen Servertypen hängt von der Systemkonfiguration ab. Möglich sind:
- Server für IBM SPSS Collaboration and Deployment Services Repository
- Verwaltete IBM SPSS Modeler-Server
- Verwaltete IBM SPSS Statistics-Server
- Verwaltete Server für IBM SPSS Modeler Text Analytics

Auswählen des Typs für einen verwalteten Server

Gehen Sie im Dialogfeld **Typ des verwalteten Servers auswählen** 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 Server** wird geöffnet.

Informationen zum verwalteten Server:

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

Bei einem Server für IBM SPSS Collaboration and Deployment Services Repository können Sie die Server-URL angeben.

Die URL enthält die folgenden Elemente:

- Das Verbindungsschema oder Protokoll als *HTTP* für Hypertext Transfer Protocol oder *HTTPS* für Hypertext Transfer Protocol mit SSL (Secure Socket Layer)
- Den Namen des Host-Servers oder die IP-Adresse

  Anmerkung: Eine IPv6-Adresse muss in eckige Klammern eingeschlossen werden, z. B. `[3ffe:2a00:100:7031::1]`.
- Die Portnummer. Wenn der Repository-Server den Standardport (Port 80 für HTTP oder Port 443 für HTTPS) verwendet, ist die Portnummer optional.
- Ein optionaler benutzerdefinierter Kontextpfad für den Repository-Server

Tabelle 2. Beispiele für URL-Spezifikationen. In dieser Tabelle werden einige Beispiele für URL-Spezifikationen für Serververbindungen aufgelistet.

URL	Schema	Host	Port	Benutzerdefinierter Pfad
`http://meinServer`	HTTP	*meinServer*	Standard (80)	(ohne)
`https://9.30.86.11:443/spss`	HTTPS	9.30.86.11	443	*spss*
`http://[3ffe:2a00:100:7031::1]:9080/ibm/cds`	HTTP	`3ffe:2a00:100:7031::1`	9080	*ibm/cds*

Wenden Sie sich an Ihren Systemadministrator, wenn Sie nicht sicher sind, welche URL Sie für Ihren Server verwenden sollen.

Bei anderen Servertypen umfassen die verfügbaren Eigenschaften die folgenden Elemente:

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

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

- Anführungszeichen (einfach und doppelt)
- Et-Zeichen (&)
- Kleiner-als- (<) und Größer-als-Zeichen (>)
- Schrägstrich (/)
- Punkte
- Kommas
- Semikolons

Port Die für die Serververbindung verwendete Portnummer.

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

Nachdem Sie die Eigenschaften definiert haben, wird der neue Server in die Liste der verwalteten Server in der Registerkarte "Serveradministration" aufgenommen.

Anzeigen von Eigenschaften des verwalteten Servers

Um die Eigenschaften eines bestehenden verwalteten Servers anzuzeigen, klicken Sie mit der rechten Maustaste auf die Registerkarte "Serveradministration" und wählen Sie **Eigenschaften** aus dem Dropdown-Menü aus.

Die angezeigten Eigenschaften hängen vom Typ des ausgewählten Servers ab.

Herstellen der Verbindung zu verwalteten Servern

Für die meisten Server müssen Sie die Verbindung in der Liste der verwalteten Server herstellen, um Verwaltungsaufgaben auszuführen. Doppelklicken Sie auf der Registerkarte "Serveradministration" auf den Server, den Sie verwalten möchten.

Anmeldung beim Server für IBM SPSS Collaboration and Deployment Services Repository

Anmeldeparameter für Repository-Server:

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

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

Provider. Der Provider, für den die angegebene Kombination aus Benutzer-ID/Kennwort für die Anmeldung geprüft werden muss. Dieses Feld wird nur angezeigt, wenn mehrere Sicherheitsprovider für das System aktiviert sind. Andernfalls validiert das System die angegebenen Berechtigungsnachweise im lokalen Benutzer-Repository.

Trennen der Verbindung zu verwalteten Servern

Melden Sie sich am Server ab, wenn Sie Ihre administrativen Aufgaben abgeschlossen haben.

1. Klicken Sie auf der Registerkarte "Serveradministration" mit der rechten Maustaste auf den Server.
2. Wählen Sie **Abmelden** aus.

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 auf der Registerkarte "Serveradministration" 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 aus.

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 zulässig. 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 Benutzer von IBM SPSS Collaboration and Deployment Services ist eine Person oder ein Prozess mit der Erlaubnis, auf Dateien zuzugreifen und Programme auszuführen. Der Benutzer wird mit einer Kombination aus Benutzername und Kennwort 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. Weitere Informationen finden Sie im Thema „Überblick über Rollen" auf Seite 25.

Benutzer und Gruppen von IBM SPSS Collaboration and Deployment Services werden von *Sicherheitsprovidern* verwaltet. Ein Sicherheitsprovider ist das System, das die Benutzerberechtigungsnachweise authentifiziert. Benutzer und Gruppen können lokal definiert werden (in diesem Fall ist IBM SPSS Collaboration and Deployment Services der Sicherheitsprovider) oder aus einem fernen Verzeichnis wie Windows Active Directory oder OpenLDAP abgeleitet werden. Weitere Informationen finden Sie in Kapitel 7, „Sicherheitsprovider", auf Seite 31.

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

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

Einrichten von Benutzern für IBM SPSS Collaboration and Deployment Services

Das Einrichten von lokalen Benutzern in IBM SPSS Collaboration and Deployment Services umfasst Folgendes:

1. Erstellen des Benutzers und gegebenenfalls Zuweisung der Gruppenmitgliedschaft. Lokale Benutzer und Gruppen können durch IBM SPSS Deployment Manager verwaltet werden.
2. Das Definieren der Zugriffsebene für den Benutzer durch Zuweisen der Rolle auf Benutzer- oder Gruppenbasis. Weitere Informationen finden Sie im Thema „Bearbeiten von Benutzern und Gruppen, die einer Rolle zugewiesen sind" auf Seite 28. Wenn die Rolle mit den geeigneten festgelegten Aktionen nicht vorhanden ist, muss sie eingerichtet werden. Weitere Informationen finden Sie im Thema „Erstellen einer neuen Rolle" auf Seite 27.

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

1. Einrichten des externen Sicherheitsproviders, falls dieser noch nicht definiert wurde. Der Benutzer wird aus diesem Sicherheitsprovider abgeleitet. Weitere Informationen finden Sie im Thema „Konfigurieren von Sicherheitsprovidern" auf Seite 32.
2. Das Erstellen berechtigter Benutzer, wenn der Zugriff auf einen untergeordneten Bereich des Active Directory auf lokal überschriebene Benutzer beschränkt werden muss. Berechtigte Benutzer können nur mit IBM SPSS 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 im fernen Verzeichnis nicht vorhanden ist. Erweiterte Gruppen können nur mit IBM SPSS Deployment Manager erstellt werden.
4. Zuweisen der Rolle auf Benutzer- oder Gruppenbasis. Rollen werden über Fernzugriff definierten Benutzern auf dieselbe Weise wie lokalen Benutzern zugewiesen.

Verwalten von Benutzern und Gruppen in IBM SPSS Deployment Manager

IBM SPSS Deployment Manager ermöglicht es Ihnen, lokale Benutzer und Gruppen sowie berechtigte Benutzer und erweiterte Gruppen zu verwalten, die für das Active Directory mit lokal überschriebenem Sicherheitsprovider definiert sind.

Bevor Sie Aktionen mit Benutzern oder Gruppen ausführen, navigieren Sie zur Verwaltungsschnittstelle, die diese Bereiche steuert.

1. Wählen Sie "Serveradministration" im Menü **Extras** aus.
2. Melden Sie sich auf der Registerkarte "Serveradministration" bei einem Server für IBM SPSS Collaboration and Deployment Services Repository an. Doppelklicken Sie auf das Symbol **Benutzer und Gruppen**, um die Hierarchie zu erweitern. Wenn keine externen Sicherheitsprovider eingerichtet sind, ist "Lokales Benutzerrepository" der einzige Eintrag in der Hierarchie. Wenn Active Directory mit lokalem Überschreiben als Sicherheitsprovider mit der Option für berechtigte Benutzer oder erweiterte Gruppen konfiguriert wurde, wird auch der Eintrag "Active Directory mit lokalem Überschreiben" angezeigt.
3. Doppelklicken Sie auf das Symbol **Lokales Benutzerrepository** oder **Active Directory mit lokalem Überschreiben**.

Der Editor "Benutzer und Gruppen verwalten" wird geöffnet.

- Für "Lokales Benutzerrepository" 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.
- 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 berechtigte Benutzer und erweiterte Gruppen erstellen und löschen und die Eigenschaften von bestehenden Gruppen bearbeiten, wenn die Optionen für berechtigte Benutzer und erweiterte Gruppen für den Sicherheitsprovider aktiviert sind. Weitere Informationen finden Sie in Kapitel 7, „Sicherheitsprovider", auf Seite 31.

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.

Benutzername. Beim Namen muss die Groß-/Kleinschreibung nicht beachtet werden und Leerzeichen sind zulässig.

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

Bestätigen. Feld zur Bestätigung des Kennworts. Wenn die Kennwörter nicht übereinstimmen, wird eine Nachricht 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 einer Suchzeichenfolge empfohlen.

Gruppen anzeigen, die mit folgenden Zeichen beginnen. Filtert die Liste mit den verfügbaren Gruppen gemäß der eingegebenen Zeichenfolge. 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. Ordnet dem Benutzer alle Gruppen zu.

Alle entfernen. Entfernt alle angezeigten Gruppen vom Benutzer.

Für das Erstellen eines lokalen Benutzers müssen Anmeldeberechtigungsnachweise angegeben werden. Der Benutzer kann außerdem Gruppen zugeordnet werden.

1. Geben Sie im Dialogfeld "Neuen Benutzer erstellen" den Benutzernamen ein.
2. Geben Sie das Kennwort ein.
3. Bestätigen Sie das Kennwort.
4. Ordnen Sie den Benutzer bei Bedarf Gruppen zu.
5. Klicken Sie auf **OK**. Der neue Benutzer wird in der Liste im Editor "Benutzer und Gruppen verwalten" angezeigt.

Bearbeiten eines Benutzers

Gruppenzuordnungen können für lokale und berechtigte Benutzer in Active Directory mit lokalem Überschreiben bearbeitet werden. Für lokale Benutzer kann das Kennwort 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.

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

Bestätigen. Feld zur Bestätigung des Kennworts. Wenn die Kennwörter nicht übereinstimmen, wird eine Nachricht 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 einer Suchzeichenfolge empfohlen.

Gruppen anzeigen, die mit folgenden Zeichen beginnen. Filtert die Liste mit den verfügbaren Gruppen gemäß der eingegebenen Zeichenfolge. 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. Ordnet dem Benutzer alle Gruppen zu.

Alle entfernen. Entfernt alle angezeigten Gruppen vom Benutzer.

Sperren und Entsperren von Benutzern

Laut Standardeinsteller wird das Benutzerkonto eines nativen Benutzers des lokalen Benutzerrepositorys, 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 Berechtigungsnachweisen), bis die Sperre für sein Konto nach dreißig Minuten automatisch oder manuell durch einen Administrator aufgehoben wurde.

In der browserbasierten Instanz von IBM SPSS Deployment Manager gibt es im Abschnitt "Sicherheit" 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 nativen Sicherheitsproviders "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 berechtigten 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.

Gruppenname. Beim Namen muss die Groß-/Kleinschreibung nicht beachtet werden und Leerzeichen sind zulässig.

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 einer Suchzeichenfolge empfohlen.

Benutzer anzeigen, die mit folgenden Zeichen beginnen. Filtert die Liste mit den verfügbaren Gruppen gemäß der eingegebenen Zeichenfolge. 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. Ordnet alle Benutzer der Gruppe zu.

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 wird in der Liste im Editor "Benutzer und Gruppen verwalten" angezeigt.

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**.

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 einer Suchzeichenfolge empfohlen.

Benutzer anzeigen, die mit folgenden Zeichen beginnen. Filtert die Liste mit den verfügbaren Gruppen gemäß der eingegebenen Zeichenfolge. 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. Ordnet alle Benutzer der Gruppe zu.

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 in Kapitel 16, „nativestore-Schema - Referenz”, auf Seite 107.

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.
2. Wählen Sie **Benutzer und Gruppen aktualisieren** oder **Alle Benutzer und Gruppen ersetzen** aus.
   - **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.
   - **Alle 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 werden in der Liste im Editor "Benutzer und Gruppen verwalten" angezeigt.

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.

Alle verfügbaren Benutzer anzeigen. Wenn die Option "Berechtigte Benutzer" aktiviert ist, wird die Liste aller berechtigten Benutzer zurückgegeben. Wenn die Option "Berechtigte 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 einer Suchzeichenfolge empfohlen.

Benutzer anzeigen, die mit folgenden Zeichen beginnen. Filtert die Liste mit den verfügbaren Gruppen gemäß der eingegebenen Zeichenfolge. 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. Ordnet alle Benutzer der Gruppe zu.

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 wird in der Liste im Editor "Benutzer und Gruppen verwalten" angezeigt.

Erstellen eines berechtigten Benutzers

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

Benutzername. Beim Namen muss die Groß-/Kleinschreibung nicht beachtet werden und Leerzeichen sind zulässig. Beachten Sie, dass es nicht möglich ist, zu prüfen, ob der Benutzer tatsächlich im fernen Verzeichnis vorhanden ist. 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 der eingegebenen Zeichenfolge. 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. Ordnet dem Benutzer alle Gruppen zu.

Alle entfernen. Entfernt alle angezeigten Gruppen vom Benutzer.

Anmerkung: Ein berechtigter Benutzer kann nur erweiterten Gruppen zugeordnet werden, wenn erweiterte 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 berechtigten Benutzers muss der Benutzername angegeben werden. Der Benutzer kann außerdem Gruppen zugeordnet werden.

1. Geben Sie im Dialogfeld "Neuen Benutzer erstellen" den Benutzernamen ein.
2. Ordnen Sie den Benutzer bei Bedarf erweiterten Gruppen zu.
3. Klicken Sie auf **OK**. Der neue berechtigte Benutzer wird in der Liste im Editor "Benutzer und Gruppen verwalten" angezeigt.

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 zusammen mit einem Sicherheitsprovider 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.

Wenn der Benutzer mehreren Gruppen angehört, enthalten die Rollen, die diesem Benutzer zugewiesen sind (Aktionsset), alle Rollen, die dem Benutzer explizit zugewiesen sind, sowie alle Rollen, die dem Benutzer indirekt über eine Gruppenzugehörigkeit zugewiesen sind. Falls dem Benutzer oder der Gruppe verschiedene Rollen zugeordnet werden, besteht das Aktionsset 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 Sicherheitsprovider verwaltet werden; Rollen dagegen werden provider-übergreifend verwaltet.

Mithilfe des Tools "Serveradministration" von IBM SPSS 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.

Anmerkung: Wenn benutzerdefinierte Beschriftungen erstellt werden, sind Benutzerrollen, die beide Aktionen **Zugriff auf Inhalte und Ordner** und **Neueste anzeigen** umfassen, zum Anzeigen/Verwenden aller Objektversionen berechtigt, die die benutzerdefinierten Beschriftungen verwenden. Wenn benutzerdefinierte Beschriftungen erstellt werden, wird `Jeder` als Standardwert für `Principal` und `Versionen verwenden` als Wert für `Berechtigungen` festgelegt. Die Tatsache, dass `Jeder` die Fähigkeit zum Anzeigen/Verwenden vom benutzerdefinierten Beschriftungen hat, bedeutet, dass alle berechtigten IBM SPSS Collaboration and Deployment Services-Benutzer Zugriff auf alle Objekte haben, die die benutzerdefinierte Beschriftung verwenden.

Aktionen von IBM SPSS Collaboration and Deployment Services

- **Zugriff auf Inhalte und Ordner.** Zugriff auf IBM SPSS Collaboration and Deployment Services Repository.

- **Zugriff auf syndizierte Feeds.** Zugriff auf syndizierte Feeds, z. B. RSS-Feeds (RSS - Really Simple Syndication).
- **Konfiguration.** Bearbeiten der Repository-Einstellungen.
- **Modell konfigurieren.** Konfigurieren von Modellen für Scoring.
- **Abonnements erstellen.** 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.
- **Berechtigungsnachweise definieren.** Erstellen, Anzeigen und Ändern von sicheren Berechtigungsnachweisen für Anwendungsserver.
- **Benutzerdefinierte Eigenschaften definieren.** Definieren und Bearbeiten von benutzerdefinierten Eigenschaften für Objekte innerhalb des Repositorys.
- **Datenquellen definieren.** Definieren und Bearbeiten von Datenquellen.
- **Nachrichtendomänen definieren.** Definieren und Bearbeiten von Domänen für JMS-Nachrichten.
- **Hochstufungsrichtlinien definieren.** Definieren und Bearbeiten von Richtlinien (Regelsätzen) zur Hochstufung von Repository-Objekten.
- **Server-Cluster definieren.** Definieren und Bearbeiten von Ausführungsserver-Clustern.
- **Server definieren.** Definieren und Bearbeiten von Ausführungsservern.
- **Themen definieren.** Definieren und Bearbeiten der Themenhierarchie für das Repository.
- **Jobbearbeitung.** Erstellen und Bearbeiten von Jobs. Beachten Sie, dass die Sichtbarkeit von Jobs für Benutzer von deren Berechtigungen abhängt.
- **Jobausführung.** Ausführen von Jobs. 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.
- **Abonnements verwalten.** Verwalten und Löschen der Abonnements anderer Benutzer.
- **MIME-Typen.** Verwalten von MIME-Typzuordnungen für das Repository.
- **Objekte hochstufen.** Hochstufen von Repository-Objekten.
- **Repository-Index.** Erstellen eines neuen Index für den Inhalt des Repositorys.
- **Benutzerdefinierte Dialogfelder ausführen.** Ausführen benutzerdefinierter IBM SPSS Statistics-Dialogfelder.
- **Bericht dynamisch ausführen.** Ausführen dynamischer Berichte in IBM SPSS Collaboration and Deployment Services Deployment Portal.
- **Zeitpläne.** Verwalten von Jobzeitplänen.
- **Modell scoren.** Scoren von Modellen.
- **Alle Versionen anzeigen.** Anzeigen aller Versionen von (beschrifteten und nicht beschrifteten) Objekten in IBM SPSS Collaboration and Deployment Services Deployment Portal. Standardmäßig sind Benutzer lediglich zur Anzeige beschrifteter Versionen in IBM SPSS Collaboration and Deployment Services Deployment Portal berechtigt.
- **Letzte anzeigen.** Anzeigen nur der aktuellste Objektversion.
- **Arbeit übergeben.** Übergeben von Arbeit (z. B. von Berichten) zur Verarbeitung durch IBM SPSS Collaboration and Deployment Services.
- **Administration der Benutzervorgaben.** Verwalten der Vorgaben anderer Benutzer. Beachten Sie, dass Produkte von IBM SPSS Collaboration and Deployment Services keine Benutzerschnittstellen zur Bearbeitung der Vorgaben anderer Benutzer aufweisen. Diese Einstellung gilt nur, wenn der Web-Service für Benutzervorgaben direkt aufgerufen wird.
- **Abgelaufene Dateien anzeigen.** Anzeigen von abgelaufenen Inhalten, wie z. B. Dateien und Jobs.

- **Modellverwaltungsdashboard anzeigen.** Anzeigen von Modelverwaltungsdashboards in IBM SPSS Deployment Manager und IBM SPSS Collaboration and Deployment Services Deployment Portal.

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

Administratorrolle

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 ein Subset an Aktionen benötigen, sollten benutzerdefinierten Rollen zugewiesen werden. Weitere Informationen finden Sie im Thema „Erstellen einer neuen Rolle".

Verwalten von Rollendefinitionen

Um mit Rollen zu arbeiten, wählen Sie **Serveradministration** aus dem Menü **Extras** und anschließend einen Server für IBM SPSS Collaboration and Deployment Services Repository aus und melden Sie sich an. Klicken Sie doppelt auf das Symbol **Rollen** für den Server, um auf den Editor "Rollendefinitionen verwalten" zuzugreifen.

Alle Rollen. Zeigt eine Liste aller Rollen, die für den Sicherheitsprovider 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 aus, um die dieser Rolle zugeordneten Aktionen zu sehen.

Definition von Rollen. Zeigt eine Liste der Aktionen, die einer ausgewählten Rolle zugeordnet 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 Rolle zu erstellen, klicken Sie im Rolleneditor auf die Schaltfläche **Neue Rolle**. Eine Rolle benötigt einen Namen und eine Liste mit zugeordneten Aktionen.

Rollenname. Eine Textzeichenfolge 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 einer Rolle keine Aktionen zugeordnet.

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

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**.

Rollenname. Eine Textzeichenfolge 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 einer Rolle keine Aktionen zugeordnet.

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

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 Benutzern und Gruppen zugeordnet werden, um Zugriffsebenen zu definieren. Um einer Rolle Benutzer und Gruppen zuzuweisen, klicken Sie im Rolleneditor auf die Schaltfläche **Benutzer und Gruppen 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 Sicherheitsprovider verfügbar sind.
- **Benutzer/Gruppen anzeigen, die mit folgenden Zeichen beginnen.** Filtert die Liste mit den verfügbaren Benutzern und Gruppen gemäß den Suchoptionen.

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

Entfernen einer Rolle

So entfernen Sie eine Rolle:

1. Wählen Sie im Rolleneditor die Rolle aus, die Sie entfernen möchten.
2. Klicken Sie auf die Schaltfläche **Löschen**. Es wird ein Bestätigungsdialogfeld geöffnet.
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)

XSS (Cross Site Scripting) ist eine Lücke in der IT-Sicherheit, die häufig in Webanwendungen zu finden ist. Sie ermöglicht es Angreifern, die clientseitigen Sicherheitsmechanismen zu umgehen, die normalerweise von modernen Web-Browsern für Webinhalte implementiert werden, indem sie ein schädliches Script 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 5.0.0.0 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 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 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 **Serveradministration** im Menü **Extras** aus.
2. Melden Sie sich auf der Registerkarte "Serveradministration" 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
- Zeichenfolgen mit einfachem Text einschränken
- Reguläre Ausdrücke für Einschränkungszeichenfolge
- Zulässige Zeichenfolgen

Änderungen an XSS-Filterregeln werden sofort angewendet (kein Serverneustart 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 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 Scripts geben könnten.

Kapitel 7. Sicherheitsprovider

Ein Sicherheitsprovider gleicht die Berechtigungsnachweise, 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 Sicherheitsprovider 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 inaktiviert 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 inaktiviert werden.

  Anmerkung: OpenLDAP ist eine Open-Source-Referenzimplementierung von LDAP. Mithilfe des OpenLDAP-Providers können Sie andere Verzeichnisserver konfigurieren, die diesem Protokoll entsprechen, einschließlich IBM Security Directory Server, und auf diese zugreifen.
- **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 inaktiviert 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 berechtigte Benutzer ermöglicht. Eine erweiterte Gruppe enthält eine Liste von Benutzern aus Active Directory, ist jedoch außerhalb des Active Directory-Framework vorhanden. Ein Filter für berechtigte 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 inaktiviert werden.

Sicherheitsprovider in IBM SPSS Deployment Manager

Bevor Sie Aktionen mit Sicherheitsprovidern ausführen, navigieren Sie zur administrativen Schnittstelle, die diese Funktionalität steuert.

1. Wählen Sie **Serveradministration** im Menü **Extras** aus.
2. Melden Sie sich auf der Registerkarte **Serveradministration** bei einem Server für IBM SPSS Collaboration and Deployment Services 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 Sicherheitsproviders mit der rechten Maustaste auf **Sicherheitsprovider** und wählen Sie die Option **Neu** aus. Ein Assistent wird angezeigt. Um die Konfiguration eines bestehenden Sicherheitsanbieters zu bearbeiten, doppelklicken Sie unter **Sicherheitsprovider** auf den Namen des betreffenden Sicherheitsproviders.

Klicken Sie zum Aktivieren oder Inaktivieren von Sicherheitsprovidern auf der Registerkarte "Serververwaltung" auf den entsprechenden Sicherheitsprovider und wählen Sie **Aktivieren** bzw. **Inaktivieren** aus.

Konfigurieren von Sicherheitsprovidern

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

Details finden Sie in den folgenden Themen.

- Native
- OpenLDAP
- Active Directory
- Active Directory mit lokaler Überschreibung

Klicken Sie zum Aktivieren oder Inaktivieren von Sicherheitsprovidern auf der Registerkarte "Serververwaltung" auf den entsprechenden Sicherheitsprovider und wählen Sie **Aktivieren** bzw. **Inaktivieren** aus.

Anmerkung: Wenn Änderungen an einer bereits vorhandenen Definition des Sicherheitsproviders vorgenommen werden, werden diese erst aktiviert, wenn das Repository neu gestartet oder der Sicherheitsprovider inaktiviert und erneut aktiviert wurde. In bestimmten Fällen, beispielsweise, wenn der Domänenname für den Active Directory-Sicherheitsprovider geändert wird, müssen Benutzer und Gruppen entfernt und anschließend erneut bestimmten Rollen zugewiesen werden. Weitere Informationen finden Sie im Thema „Einrichten von Benutzern für IBM SPSS Collaboration and Deployment Services” auf Seite 17.

Native

Der native Sicherheitsprovider "Lokales Benutzer-Repository" ist ein interner Sicherheitsprovider von IBM SPSS Collaboration and Deployment Services und umfasst keine Einstellungen, die konfiguriert werden können.

OpenLDAP

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

Klicken Sie zur Konfiguration eines neuen OpenLDAP-Sicherheitsproviders mit der rechten Maustaste auf **Sicherheitsprovider** und wählen Sie folgende Optionsfolge aus:

Neu > **Sicherheitsproviderdefinition**

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

Hosteinstellungen

- **Host-URL.** Der Pfad zum LDAP-Server, in der Regel ein über 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 aus.

  Anmerkung: Wenn eine LDAPS-Adresse (LDAP über SSL) in **Host-URL** (zum Beispiel `ldaps://IhrServer.IhrUnternehmen.com`) angegeben ist, müssen Sie die Einstellung **Secured Socket Layer-Verbindung verwenden** nicht aktivieren.
- **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 Informati-

onen zum Suchsteuerelement für Paging-Ergebnisse finden Sie unter *RFC 2686 - LDAP Control Extension for Simple Paged Results Manipulation* (*http://datatracker.ietf.org/doc/rfc2696/*).

Berechtigungsnachweise

- **Berechtigungsnachweistyp suchen.** Geben Sie an, wie mit den Suchberechtigungsnachweisen 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 Suchbenutzerkennwort angeben zu müssen. Bei der Option *Kerberos-Berechtigungsnachweis verwenden* wird der Berechtigungsnachweis für die Serverprozesse des Servers für Suchvorgänge verwendet. Wählen Sie die Option *Bereitgestellte Berechtigungsnachweise verwenden* aus, um eine Benutzer-ID und ein Kennwort als Berechtigungsnachweise 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.
- **Kennwort für Benutzer der Suchfunktion.** Aus Sicherheitsgründen wird das Kennwort des Domänenbenutzers durch Sterne (*) ersetzt. Geben Sie den Wert in beide Kennwortfelder ein, um den korrekten Wert zu bestätigen.

Definition der Benutzerbindung

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

Einstellungen für die Benutzersuche

- **Basis-DN für Suchfilter.** Basis-DN (Distinguished Name) für Benutzersuchen.
- **Objektfilterausdruck.** Objektklasse und -wert für die Filterung. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Suchfilterausdruck.** Das Attribut, das als Such-ID verwendet werden soll. Dieser Wert hängt vom verwendeten LDAP-Schema ab.
- **Suche nach Attribut.** 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 Attribut, das als Such-ID verwendet werden soll. 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.
- **Zugehörigkeitsattribut.** 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-Sicherheitsproviders mit der rechten Maustaste auf **Sicherheitsprovider** und wählen Sie folgende Optionsfolge aus:

Neu > **Sicherheitsproviderdefinition**

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

Hosteinstellungen

- **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 aus.
- **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).

Berechtigungsnachweise

- **Berechtigungsnachweistyp suchen.** Geben Sie an, wie mit den Suchberechtigungsnachweisen 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 Suchbenutzerkennwort angeben zu müssen. Bei der Option *Kerberos-Berechtigungsnachweis verwenden* wird der Berechtigungsnachweis für die Serverprozesse des Servers für Suchvorgänge verwendet. Wählen Sie die Option *Bereitgestellte Berechtigungsnachweise verwenden* aus, um eine Benutzer-ID und ein Kennwort als Berechtigungsnachweise 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.
- **Kennwort für Benutzer der Suchfunktion.** Aus Sicherheitsgründen wird das Kennwort des Domänenbenutzers durch Sterne (*) ersetzt. Geben Sie den Wert in beide Kennwortfelder ein, um den korrekten Wert zu bestätigen.

Domänenname.

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

Definition der Benutzerbindung

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

Einstellungen für die Benutzersuche

- **Basis-DN für Suchfilter.** Basis-DN (Distinguished Name) für Benutzersuchen.
- **Objektfilterausdruck.** Objektklasse und -wert für die Filterung. Dieser Wert hängt vom verwendeten Schema ab.
- **Suchfilterausdruck.** Das Attribut, das als Such-ID verwendet werden soll. Dieser Wert hängt vom verwendeten Schema ab.

- **Suche nach Attribut.** 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 Attribut, das als Such-ID verwendet werden soll. 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.
- **Zugehörigkeitsattribut.** 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 Sicherheitsproviders für ein Active Directory mit lokalem Überschreiben mit der rechten Maustaste auf **Sicherheitsprovider** und wählen Sie folgende Optionsfolge:

Neu > **Sicherheitsproviderdefinition**

Der Assistent zum Erstellen einer neuen Sicherheitsproviderdefinition wird angezeigt. Wählen Sie im Dropdown-Menü **Typ** die Option **Active Directory mit lokalem Überschreiben** aus. Geben Sie einen Namen für die Sicherheitsproviderdefinition 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:

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

Sicherheitsprovider in der browserbasierten Instanz von IBM SPSS Deployment Manager

So aktivieren Sie die Seite "Sicherheitsprovider":

1. Klicken Sie in der Navigationsliste auf **Sicherheitsprovider**. Die Seite "Sicherheitsprovider" wird angezeigt.

   So ändern Sie die verwendeten Sicherheitsprovider:
2. Wählen Sie die Kontrollkästchen neben dem Sicherheitsprovider aus oder ab.
3. Klicken Sie auf **Setzen**.

Beachten Sie, dass ausschließlich Sicherheitsprovider in der Liste angezeigt werden, die zuvor im Client von IBM SPSS Deployment Manager erstellt wurden.

Aktivieren und Inaktivieren von Sicherheitsprovidern

Es werden ausschließlich Sicherheitsprovider im Browser angezeigt, die zuvor im Client von IBM SPSS Deployment Manager erstellt und konfiguriert wurden. Bei jedem Sicherheitsprovidertyp können Sie einige Einstellungen anzeigen, die für die Art des eingesetzten Authentifizierungs- und Autorisierungssys-

tems typisch sind. Verwenden Sie jedoch den Client von IBM SPSS Deployment Manager, um neue Sicherheitsprovider zu konfigurieren oder die Einstellungen insgesamt zu ändern.

Sie können die verfügbaren Sicherheitsprovider mit den Kontrollkästchen neben jedem Sicherheitsprovider und durch Klicken auf **Festlegen** aktivieren bzw. inaktivieren.

Nativ (lokal)

Der native (lokale) Sicherheitsprovider ist systeminhärent und kann nicht entfernt werden. Dem nativen Sicherheitssystem können Benutzer hinzugefügt werden, das System kann jedoch nicht inaktiviert werden.

Active Directory

Um bestimmte Active Directory-Einstellungen anzuzeigen, klicken Sie rechts neben dem Kontrollkästchen "Active Directory" auf **Einstellungen anzeigen**. Es wird ein Subset der aktuellen Einstellungen angezeigt.

Beachten Sie, dass der Active Directory-Sicherheitsprovider nur verfügbar ist, wenn dieser zuvor im Client von IBM SPSS Deployment Manager konfiguriert wurde. Informationen zu bestimmten Einstellungen finden Sie unter „Active Directory" auf Seite 34.

Active Directory mit lokaler Überschreibung

Über die Sicherheitsprovideroption "Active Directory mit lokalem Überschreiben" kann Active Directory mit den zusätzlichen Optionen eines lokalen Principalfilters 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 ein Subset 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-Sicherheitsprovider mit lokalem Überschreiben nur verfügbar ist, wenn dieser zuvor im Client von IBM SPSS Deployment Manager konfiguriert wurde.

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

OpenLDAP

Um bestimmte OpenLDAP-Einstellungen anzuzeigen, klicken Sie rechts neben dem Kontrollkästchen "OpenLDAP" auf **Einstellungen anzeigen**. Es wird ein Subset der aktuellen Einstellungen angezeigt. Beachten Sie, dass der OpenLDAP-Sicherheitsprovider nur verfügbar ist, wenn dieser zuvor im Client von IBM SPSS Deployment Manager konfiguriert wurde. Informationen zu bestimmten Einstellungen finden Sie unter „OpenLDAP" auf Seite 32.

Kapitel 8. Single Sign-on

Single Sign-on (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 Single-Sign-on-Funktionalität, indem Benutzer beim ersten Mal über einen externen Verzeichnisservice basierend auf dem *Kerberos*-Sicherheitsprotokoll authentifiziert werden. Anschließend werden die Berechtigungsnachweise in allen Anwendungen von IBM SPSS Collaboration and Deployment Services (zum Beispiel IBM SPSS Deployment Manager, IBM SPSS Collaboration and Deployment Services Deployment Portal oder einem Portalserver) ohne eine weitere Authentifizierung verwendet.

Die Konfiguration für Single Sign-on wird in der Registerkarte "Serveradministration" von IBM SPSS Deployment Manager ausgeführt. Beachten Sie, dass eine Reihe von Voraussetzungen erfüllt sein müsen, bevor Single Sign-on aktiviert werden kann. Weitere Informationen zur Installation und Konfiguration finden Sie in der Dokumentation zu IBM SPSS Collaboration and Deployment Services.

Konfigurieren von Single Sign-on

1. Wählen Sie **Serveradministration** aus dem Menü **Extras** aus, melden Sie sich an einem Server für IBM SPSS Collaboration and Deployment Services an und klicken Sie doppelt auf das Symbol **Single Sign-On**. Der Editor für Single Sign-on-Provider wird geöffnet.

- **Aktivieren.** Aktiviert oder inaktiviert die Verwendung von Single-Sign-on-Provider.
- **Sicherheitsprovider.** Ein konfigurierter externer Sicherheitsprovider, wie Windows Active Directory. Lokale Sicherheitsprovider können nicht ausgewählt werden.
- **Hostadresse 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 Hosts für IBM SPSS Collaboration and Deployment Services Repository. Beispiel: `repositoryhost.mycompany.com`.
- **Kerberos-Service-Principal-Name.** Der Benutzername für den Kerberos-Service-Principal.
- **Kerberos-Service-Principal-Kennwort.** Das Kennwort für den Kerberos-Service-Principal.
- **URL für Kerberos-Schlüsseltabelle.** Die URL zur Chiffrierschlüsseldatei für die Kerberos-Principal-Authentifizierung.
- **JAAS-Konfigurationsdatei.** Der Pfad der JAAS-Konfigurationsdatei (Java Authentication and Authorization Service) auf dem Hostdateisystem von IBM SPSS Collaboration and Deployment Services. 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 Benutzerschnittstelle verwendet werden, bis hin zu den Nachrichten reichen, die im Anmeldungsfenster angezeigt werden.

Führen Sie folgende Schritte in der browserbasierten Instanz von IBM SPSS Deployment Manager aus, um auf diese Optionen zuzugreifen:

1. Klicken Sie in **Konfiguration** in der Navigationsliste. Die Konfigurationsseite wird geöffnet.
2. 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 Konfigurationsoptionen sind für optionale Komponenten von IBM SPSS Collaboration and Deployment Services oder für andere IBM SPSS-Produkte vorgesehen, wie beispielsweise IBM SPSS Statistics oder IBM ShowCase. Die Optionen sind nur verfügbar, wenn die Komponenten installiert sind.

Administrator

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

So bearbeiten Sie das Vorlagenverzeichnis:

1. Klicken Sie in der Konfigurationsliste unter "Administrator" auf **Vorlagen**. Das aktuelle Vorlagenverzeichnis wird im Textfeld "Vorlagen" angezeigt.
2. Geben Sie im Textfeld "Vorlagen" den neuen Pfad des Verzeichnisses ein, das die Vorlagen enthält, die Sie verwenden möchten.
3. Klicken Sie auf **Setzen**. Der von Ihnen angegebene Pfad wird zum Standardpfad für den Zugriff des Systems auf Vorlagen.
4. 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.

Prozesskoordinator

Die Konfigurationsoptionen für den Prozesskoordinator (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 3. Konfigurationsoptionen für den Prozesskoordinator.

Name	Beschreibung	Einstellungen
Zeitlimitüberschreitung für anstehende Verbindung	Das Ablaufzeitlimit für anstehende Verbindungsanforderungen. Der Prozesskoordinator löscht eine Verbindungsanforderung, wenn der Zielserver nicht innerhalb des angegebenen Zeitintervalls antwortet.	Ganzzahl. Die Standardeinstellung lautet 5 (Sekunden).
Wartungsprovider für Prozesskoordinator aktiviert	Aktiviert bzw. inaktiviert 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 4. Konfigurationsoptionen für benutzerdefinierte Dialogfelder.

Name	Beschreibung	Einstellungen
Durchsuchen des Dateiservers aktiviert	Legt fest, ob bei der Auswahl eines Datasets für einen benutzerdefinierten Dialog das Durchsuchen nach IBM SPSS Statistics-Datasets 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 Datasets für ein benutzerdefiniertes Dialogfeld für das Durchsuchen nach IBM SPSS Statistics-Datasets verwendet wird. Wenn das Durchsuchen des Dateiservers aktiviert und kein Speicherort angegeben ist, wird das Dateisystem des angegebenen IBM SPSS Statistics-Servers verwendet.	Bei dem Wert kann es sich um einen Netzpfad oder um den absoluten Pfad eines Verzeichnisses handeln.
Name des Dateiservers	Der Name, der dem für das Durchsuchen nach IBM SPSS Statistics-Datasets zu verwendenden Dateiserver zugewiesen werden soll.	Ein Zeichenfolgewert (Zeichenfolge). Wenn kein Wert angegeben ist, wird der Name "File Server" verwendet.
Durchsuchen des Repositorys aktiviert	Legt fest, ob bei der Auswahl eines Datasets für einen benutzerdefinierten Dialog das Durchsuchen nach IBM SPSS Statistics-Datasets im Repository aktiviert ist.	Standardmäßig aktiviert.

Tabelle 4. Konfigurationsoptionen für benutzerdefinierte Dialogfelder (Forts.).

Name	Beschreibung	Einstellungen
IBM SPSS Statistics-Server	Der Repository-Name oder URI eines IBM 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 Zeichenfolge, 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 Dokumentation zu IBM SPSS Deployment Manager.
IBM SPSS Statistics-Serverberechtigungsnachweise	Die Berechtigungsnachweise, über die eine Verbindung zu dem IBM SPSS Statistics-Server hergestellt wird, wenn Syntax für ein benutzerdefiniertes Dialogfeld ausgeführt wird. *Hinweis*: Der Berechtigungsnachweis ist nicht erforderlich, wenn Active Directory zur Verwendung mit IBM SPSS Collaboration and Deployment Services konfiguriert wurde.	Eine Zeichenfolge, die dem Repository-Namen oder URI des Berechtigungsnachweisobjekts entspricht.
IBM SPSS Statistics-Sitzungszeitlimitüberschreitung	Legt den Zeitlimitüberschreitungswert in Minuten fest, der angibt, wie lange eine Verbindung zum IBM SPSS Statistics-Server aufrechterhalten werden soll, wenn keine Aktivität seitens eines Benutzers erfolgt.	Ganzzahl. Die Standardeinstellung lautet 20 (Minuten).

Datenservice

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

Wichtig: Die folgenden Optionen können in der Konfiguration angezeigt werden, auch wenn die Datenservicefunktion nicht mehr unterstützt wird oder nicht mehr auf sie zugegriffen werden kann.

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 5. Konfigurationsoptionen für den Datenservice.

Name	Beschreibung	Einstellungen
Aktive Verbindungen - maximale Anzahl	Maximale Anzahl an aktiven Verbindungen.	Ganzzahl. Der Standardwert ist 5.
Inaktive Verbindungen - maximale Anzahl	Maximale Anzahl an inaktiven Verbindungen.	Ganzzahl. Der Standardwert ist 5.

Tabelle 5. Konfigurationsoptionen für den Datenservice (Forts.).

Name	Beschreibung	Einstellungen
Maximum Quellenzeilen	Maximale Anzahl der Datensätze, die bei der Ausführung eines Echtzeitdatenzugriffsplans standardmäßig für jeden Quellenknoten abgerufen werden sollen. Werden mehr Datensätze angefordert als von diesem Wert angegeben, schlägt der Datenabruf fehl. Dieser Wert wird für alle Quellenknoten in einem Datenzugriffsplan verwendet, für die kein Grenzwert für Zahl der Datensätze angegeben wurde.	Ganzzahl

Deployment Manager

Die Konfigurationsoption für Deployment Manager ermöglicht es Ihnen, das Protokollzeitlimit für die Kommunikation zwischen IBM SPSS Deployment Manager und dem Repository anzugeben.

Geben Sie die Zeit, die der Client von IBM SPSS Deployment Manager auf einen Repository-Server warten soll, in Sekunden an. Verwenden Sie einen höheren Wert, wenn bei Servertransaktionen Fehlernachrichten gegeben werden.

Bearbeiten des Protokollzeitlimits

1. Klicken Sie in der Konfigurationsliste unter "Deployment Manager" auf **Zeitlimitüberschreitung für Protokoll**. Der aktuelle Wert wird angezeigt.
2. Geben Sie die Anzahl von Sekunden im Textfeld "Zeitlimitüberschreitung für Protokoll" ein.
3. Klicken Sie auf **Setzen**. Der von Ihnen angegebene Wert wird als Zeitlimit übernommen.
4. 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

Mithilfe der Konfigurationsoptionen für Deployment Portal können Sie Authentifizierungseinstellungen für die webbasierte Anwendung von IBM SPSS Collaboration and Deployment Services Deployment Portal angeben.

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 6. Konfigurationsoptionen für IBM SPSS Collaboration and Deployment Services Deployment Portal.

Name	Beschreibung	Einstellungen
Konfigurierte Authentifizierungskriterienklasse	Der Name der Java-Klasse, der verwendet wird, um Authentifizierungsinformationen für die Anwendung von IBM SPSS Collaboration and Deployment Services Deployment Portal 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 IBM SPSS Collaboration and Deployment Services 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 IBM SPSS Collaboration and Deployment Services Deployment Portal weiterzugeben und so die Anmeldemaske zu umgehen.	Standardmäßig inaktiviert.

Deployment Portal-Scoring

Mit der Konfigurationsoption "Zeilenbegrenzung für Stapelscoring" können Sie die maximale Anzahl von Zeilen angeben, die beim Stapelscoring aus einem ausgewählten Dataset verwendet wird.

So ändern Sie die Zeilenbegrenzung:

1. Klicken Sie in der Konfigurationsliste unter "Deployment Portal-Scoring" auf **Zeilenbegrenzung für Stapelscoring**. Der aktuelle Wert wird angezeigt.
2. Geben Sie im Textfeld "Zeilenbegrenzung für Stapelscoring" die Zeilenanzahl ein.
3. Klicken Sie auf **Setzen**. Der von Ihnen angegebene Wert wird als Zeilenbegrenzung verwendet.
4. 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 Konfigurationsoptionen für Enterprise-Ansicht 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 7. Konfigurationsoptionen für IBM SPSS Collaboration and Deployment Services Enterprise View.

Name	Beschreibung	Einstellungen
Maximale CQL-Abfragespalten	Die maximale Zeilenzahl, die von CQL (Common Query Language)-Abfragen zurückgegeben wird.	Ganzzahl. Der Standardwert ist 2.
Zusätzliche IBM SPSS Statistics-Datendatei-Server	Mithilfe dieser Einstellung werden zusätzliche IBM SPSS Statistics-Datendatei-Server angegeben, mit denen sich Metadaten aus IBM SPSS Statistics-Datendateien abrufen lassen.	Eine durch Semikolon getrennte Liste mit `Host:Port`-Werten, z. B. `server2:18886;server3:18886`

Tabelle 7. Konfigurationsoptionen für IBM SPSS Collaboration and Deployment Services Enterprise View (Forts.).

Name	Beschreibung	Einstellungen
IBM SPSS Statistics-Datendatei-Lastausgleich	Die Lastausgleichseinstellung steuert, ob beim Abruf von Metadaten aus IBM SPSS Statistics-Datendateien mehrere IBM SPSS Statistics-Datendatei-Server im ausfallsicheren Modus oder Lastausgleichsmodus verwendet werden. Im ausfallsicheren Modus werden die Listenserver in sequenzieller Reihenfolge verwendet. Wenn der erste nicht funktioniert, wird der zweite verwendet usw. Wenn der Lastausgleich aktiviert wird, wird einer der verfügbaren Server nach dem Zufallsprinzip ausgewählt. Diese Einstellung hat keine Wirkung, sofern keine zusätzlichen IBM SPSS Statistics-Datendatei-Server angegeben werden.	Standardmäßig aktiviert.
IBM SPSS Statistics-Datendatei-Server-Host	Der Name des IBM SPSS Statistics-Datendatei-Servers, der zum Zugriff auf IBM SPSS Statistics-Datendateien verwendet wird. Falls kein Host angegeben ist, wird localhost verwendet.	Eine gültige IP-Adresse bzw. ein gültiger Hostname.
IBM SPSS Statistics-Datendatei-Server-Port	Der Port für den IBM SPSS Statistics-Datendatei-Server. Falls kein Port angegeben ist, wird der Standard-Port verwendet.	Eine gültige Portnummer.
IBM SPSS Statistics-Datendatei-Server Secure	Indikator, ob bei der Kommunikation mit dem IBM SPSS Statistics-Datendatei-Server SSL verwendet werden soll oder nicht. Der Standardwert "falsch" heißt, dass keine Secure Sockets verwendet werden.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".

Hilfe

Die Konfigurationsoptionen für die Hilfe ermöglichen es Ihnen, den Speicherort der Dokumentationskomponenten für die browserbasierte Instanz von IBM SPSS Deployment Manager anzugeben.

Standardmäßig verwendet das System die vom Installationsprogramm festgelegten Pfade. In der Tabelle Tabelle 8 sind die verfügbaren Einstellungen beschrieben.

Tabelle 8. Konfigurationsoptionen für die Hilfe.

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

Weitere Informationen finden Sie im Thema „Optimieren der Leistung des Benachrichtigungsservice" auf Seite 82. Sie können auch Syndikationseinstellungen 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. Konfigurationsoptionen für Benachrichtigungen.

Name	Beschreibung	Einstellungen
Binärer Inhalt aktiviert	Aktiviert binäre Inhalte, z. B. E-Mail-Anhänge, für Hinweisnachrichten.	Standardmäßig aktiviert.
Größe des Sammlungspools für Core-Ereignisse	Anzahl der Threads, die im Ereignissammlungspool bleiben, auch wenn sie inaktiv sind.	Ganzzahl. Der Standardwert ist 16.
Distinkte Empfänger	Falls das Kontrollkästchen aktiviert ist, werden Hinweisnachrichten nur für eindeutige Empfänger generiert. Andernfalls werden die doppelten Adressen nicht entfernt und die Empfänger erhalten Nachrichten, die von all ihren einzelnen Abonnements und Benachrichtigungen generiert wurden, die dem bestimmten Benachrichtigungsereignis entsprechen. Diese Option sollte nur zu Debugzwecken 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. Der Standardwert ist 32.
Ereignisvererbung aktiviert	Definiert, ob abgeleitete Benachrichtigungsereignisse durch den Service verarbeitet werden sollen.	Standardmäßig inaktiviert.

Tabelle 9. Konfigurationsoptionen für Benachrichtigungen (Forts.).

Name	Beschreibung	Einstellungen
Ereignisfilter	Filtert Benachrichtigungsereignisse heraus, die zu einem frühen Zeitpunkt im Prozess über keine entsprechenden Abonnements bei zugehörigen Benachrichtigungsprovidern 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. Der Standardwert ist 2048.
Zeichenfolgeschlüssel für Ereignisfilter	Verwendet Zeichenfolgen anstelle von Hash-Codes zur Identifizierung von Benachrichtigungsereignissen.	Standardmäßig inaktiviert.
Festschreibungsstapelgröße für Ereigniswarteschlangenspeicher	Legt die Festschreibungsstapelgröße des persistenten Speichers für die ankommenden Benachrichtigungsereignisse fest. Der Benachrichtigungsservice muss neu gestartet werden, damit die Änderungen wirksam werden.	Ganzzahl. Der Standardwert ist 32.
Maximale Größe des Sammlungspools für Core-Ereignisse	Die maximal zulässige Anzahl an Threads im Ereignissammlungspool.	Ganzzahl. Der Standardwert ist 32.
Nachrichtenbus aktiviert	Definiert, ob Hinweisnachrichten an den JMS-Nachrichtenbus gesendet werden sollen.	Standardmäßig aktiviert.
Nachrichtenbusfilter aktiviert	Definiert, ob nur Benachrichtigungen von Interesse an den JMS-Nachrichtenbus gesendet werden sollen.	Standardmäßig aktiviert.
Benachrichtigungsauditor aktiviert	Legt fest, ob der Benachrichtigungsservice mit dem Auditing-Service verknüpft werden soll.	Standardmäßig aktiviert.
Benachrichtigungscache verteilt	Legt fest, ob der Benachrichtigungsservice einen verteilten Cache verwenden soll. Der Benachrichtigungsservice muss neu gestartet werden, damit die Änderungen wirksam werden.	Standardmäßig inaktiviert.
Warteschlange für Benachrichtigungen	Stellt ankommende Benachrichtigungsereignisse in die Warteschlange, bis sie durch Hintergrund-Threads verarbeitet werden können.	Wahr oder Falsch. Die Standardeinstellung lautet "wahr".
Persistente Ereigniswarteschlange aktiviert	Definiert, ob eingehende Benachrichtigungsereignisse temporär im persistenten Speicher auf dem Datenträger bleiben sollen, um die Menge des belegten Speichers zu minimieren. Der Benachrichtigungsservice muss neu gestartet werden, damit die Änderungen wirksam werden.	Standardmäßig inaktiviert.
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.

Tabelle 9. Konfigurationsoptionen für Benachrichtigungen (Forts.).

Name	Beschreibung	Einstellungen
Typ der persistenten Ereigniswarteschlange	Definiert den Speichertyp für die persistente Ereigniswarteschlange. Der Benachrichtigungsservice muss neu gestartet werden, damit die Änderungen wirksam werden.	Entweder `DISK` oder `JMS`. Standard ist `DISK`.
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 bereitstellungs- 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 bereitstellungs- 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 abgewählt 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"-Codierungen in "8bit"-Codierung konvertiert, falls sie die RFC2045-Regeln für 8-Bit-Text einhalten.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".
SMTP-Authentifizierung	Wenn die Option auf "wahr" gesetzt ist, wird versucht, den Benutzer mithilfe des Befehls `AUTH` zu authentifizieren.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".
Zeitlimit für SMTP-Verbindung	Zeitlimit für Socketverbindung in Millisekunden.	Ganzzahl. Standardmäßig ist das Zeitlimit unendlich.
SMTP-Distributor aktiviert	Wenn dieses Kontrollkästchen aktiviert ist, ist eine Verteilung von Hinweisnachrichten über SMTP möglich. Der Repository-Administrator kann die SMTP-Verteilung inaktivieren, um alle vom Server generierten E-Mails zu unterdrücken. Beachten Sie, dass bei inaktivierter 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).

Tabelle 9. Konfigurationsoptionen für Benachrichtigungen (Forts.).

Name	Beschreibung	Einstellungen
SMTP DSN RET	Die Option `RET` für den Befehl `MAIL` für DSN (Delivery Status Notifications, RFC3461).	Entweder `FULL` oder `HDRS`.
SMTP EHLO	Wenn "falsch" eingestellt ist, wird nicht versucht, eine Anmeldung mit dem `EHLO`-Befehl durchzuführen.	Wahr oder Falsch. Die Standardeinstellung lautet "wahr".
SMTP aus E-Mail-Adresse	Absender- oder Antwortadresse bei der Verwendung für Benachrichtigungs-E-Mails.	Eine vorhandene SMTP-E-Mail-Adresse.
SMTP-Host	Der Hostname bzw. die IP-Adresse des SMTP-Servers, der zum Versenden von Mails verwendet wird.	Eine gültige IP-Adresse bzw. ein gültiger Hostname.
Lokaler SMTP-Host	Name des lokalen Hosts, der im SMTP-Befehl `HELO` oder `EHLO` verwendet wird. Verwendet standardmäßig *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	Kennwort für die SMTP-Authentifizierung.	Maskiertes Kennwort.
SMTP-Port	Der Port, der für ausgehende Mails verwendet wird.	Eine gültige Portnummer. Der Standardwert ist 25.
SMTP QUIT	Wenn diese Option auf "wahr" eingestellt ist, wartet der Transport die Antwort auf den Befehl `QUIT` ab. Wenn diese Option auf "falsch" eingestellt ist, wird der Befehl `QUIT` gesendet und die Verbindung sofort geschlossen.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".
SMTP SASL-Gebiet	Das SASL-Gebiet (Simple Authentication and Security Layer) zur Verwendung mit DIGEST-MD5-Authentifizierung.	Eine bereitstellungs- oder serverspezifische Zeichenfolge, die das Gebiet oder die Domäne kennzeichnet, aus dem/der der Name des Principals 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 Nachricht dennoch gesendet und der teilweise Misserfolg durch eine *SendFailedException* gemeldet. Wenn die Option auf "falsch" eingestellt ist, wird die Nachricht an keinen der Empfänger gesendet, wenn eine oder mehrere der Empfängeradressen ungültig sind.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".
SMTP-Zeitlimitüberschreitung	Zeitbegrenzungswert für Socket-E/A in Millisekunden.	Ganzzahl. Standardmäßig ist das Zeitlimit unendlich.
SMTP-Transferprotokoll	Nachrichtentransferprotokoll.	Entweder `smtp` oder `smtps`. Der Standardwert lautet `smtp`, während `smtps` für Verbindungen zum entsprechenden Service über SSL/TLS verwendet wird.
SMPT - Debugmodus einschalten	Schaltet den Debugmodus ein und aus.	Wahr oder Falsch. Die Standardeinstellung ist "falsch".

Tabelle 9. Konfigurationsoptionen für Benachrichtigungen (Forts.).

Name	Beschreibung	Einstellungen
SMTP-Benutzer	Standardbenutzername für SMTP.	Benutzername.
Abonnement-ID-Cache	Definiert eine maximale Größe des LRU-Cache für häufig verwendete Abonnement-IDs.	Ganzzahl. Der Standardwert ist 2048.
Cache-TTL für syndizierte Einträge	Definiert die Zeitspanne, für die syndizierte 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 syndizierte Einträge	Definiert die maximale Anzahl an Einträgen in syndizierten Feeds wie RSS-Feeds.	Ganzzahl. Der Standardwert ist 256.
Persistente TTL für syndizierte Einträge	Definiert die Zeitspanne, für die syndizierte Einträge im persistenten Speicher abgelegt werden (in Tagen). Dies bezieht sich beispielsweise auf Feeds vom Typ RSS.	Ganzzahl. Die Standardeinstellung lautet 7 Tage.
Typ der gesammelten Feeds	Definiert das Format der syndizierten 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 syndizierte 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 syndizierte 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 Inaktivieren 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. Der Standardwert ist 60 Minuten.
Syndication Vacuumer – Master	Definiert, ob Syndication Vacuumer nur auf dem Masterknoten im Server-Cluster ausgeführt wird.	Standardmäßig inaktiviert.
Syndication Vacuumer-Quote	Schränkt die Anzahl der syndizierten Einträge ein, die während einer einzelnen Ausführung von Syndication Vacuumer gelöscht werden.	Ganzzahl. Der Standardwert ist 4096.
Größe des Datenträgercache für Datenquelle	Maximale Größe des Datenträgercache für binäre Inhalte (Anhänge), die als Teil eines Benachrichtigungsereignisses gesendet werden.	Ganzzahl. Der Standardwert ist 64.

Pager

Über die Konfigurationsoption für Pager-Zeitlimitüberschreitungen 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.

Wichtig: Ein Neustart des Repositorys ist nötig, damit der neue Optionswert wirksam wird.

Bearbeiten der des Pagerzeitlimits

1. Klicken Sie in der Konfigurationsliste unter "Pager" auf **Pager-Zeitlimitüberschreitung**. Der aktuelle Wert wird angezeigt.
2. Geben Sie die Anzahl von Minuten im Textfeld "Pager-Zeitlimitüberschreitung" ein.
3. Klicken Sie auf **Setzen**. Der von Ihnen angegebene Wert wird als Zeitlimit übernommen.
4. 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 Konfigurationsoptionen für das Prozessmanagement ermöglichen es Ihnen, Jobausführungseinstellungen anzugeben und die Web-Service-Endpunkte für das Prozessmanagement 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 10. Konfigurationsoptionen für das Prozessmanagement.

Name	Beschreibung	Einstellungen
Kalenderpool	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. Der Standardwert ist 60.
Hash-bang-Shellpfad	Gibt die Hash-bang-Kombination (#!) für die erste Zeile des UNIX-Scripts an, gefolgt vom Pfadnamen der Shell, die das Script ausführt.	
Name der JMS Connection Factory	Der Name, der für die JMS Connection Factory beim JNDI-Service registriert ist. Ziehen Sie die Dokumentation zu Ihrem Anwendungsserver oder JMS-Server zu Rate, um den angemessenen Wert zu ermitteln.	Der Standardwert ist `ConnectionFactory`. Der Name muss innerhalb des zugehörigen Messaging-Providers eindeutig sein.
JMS Naming Factory	Die JMS-Java-Klasse. Beispielsweise ist die Naming-Factory für den JBoss-Anwendungsserver *org.jnp.interfaces.NamingContextFactory*. Die Einstellung kann festgelegt werden, wenn alle Nachrichten für alle nachrichtenbasierten Jobs von einem einzigen fernen Server stammen.	Der Standardwert ist der Klassenname der JMS Naming Factory des lokalen Anwendungsservers.

Tabelle 10. Konfigurationsoptionen für das Prozessmanagement (Forts.).

Name	Beschreibung	Einstellungen
JMS Naming Service	Der URI-Speicherort des Naming-Service. Zum Beispiel ist die Naming-Factory für den JBoss-Anwendungsserver `jnp://localhost:1099`. Die Einstellung kann festgelegt werden, wenn alle Nachrichten für alle nachrichtenbasierten Jobs von einem einzigen fernen 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. Der Standardwert ist 10.
Abfragemetriken protokollieren	Gibt an, ob die Abfragemetriken (Laufzeit) im Protokoll aufgezeichnet werden sollen.	Standardmäßig inaktiviert.
Maximale Anzahl an Iterationen	Die maximale Anzahl von Iterationen für iterative Jobschritte.	Ganzzahl. Der Standardwert ist 250.
Nachrichtenabfrage	Die Wartezeit (in Sekunden), bevor der Process Management-Server das Repository erneut nach nachrichtenbasierten Zeitplänen absucht, die aktiviert werden sollten.	Ganzzahl. Der Standardwert ist 120.
Modeler-Sync	Definiert, ob die gleichzeitige Ausführung von Jobs, die IBM SPSS Modeler-Dateien enthalten, zulässig ist.	Standardmäßig inaktiviert.
Prozessbenachrichtigung aktiviert	Gibt an, ob der Process Management-Server mit dem Benachrichtigungsserver kommunizieren soll.	Wahr oder Falsch. Die Standardeinstellung lautet "wahr".
Abfrage des Fernverarbeitungsservers	Die Wartezeit (in Sekunden), bevor die ferne Arbeit prüft, ob der Fernverarbeitungsserver noch aktiv ist	
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.

Tabelle 10. Konfigurationsoptionen für das Prozessmanagement (Forts.).

Name	Beschreibung	Einstellungen
Ablaufzeit für übergebenes Artefakt	Die Ablaufzeit (in Tagen) für übergebene Artefakte, wie beispielsweise Jobs.	Ganzzahl. Der Standardwert ist 5.
Zeitmarke für übergebenes Artefakt	Das Zeitmarkenformat, 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 Zeitmarke.	Datums- und Zeitformat für die Ordner mit Zeitmarke.	Format für Jahr, Monat, Tag, Stunde, Minute, Sekunde: `yyyy.MM.dd.hh.mm.ss.SSS`
Datumsformat für die Ordner mit Zeitmarke.	Datumsformat für die Ordner mit Zeitmarke.	Monat, Tag und Jahr: `MM-dd-yyyy`
Zeitformat für die Ordner mit Zeitmarke.	Zeitformat für die Ordner mit Zeitmarke.	Format für Stunde, Minute und Sekunde: `HH.mm.ss`

Reporting

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

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

Bearbeiten des Verzeichnispfads:

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

Repository

Die Konfigurationsoptionen für das Repository ermöglichen es Ihnen, die Web-Service-Endpunkte zu definieren und die Verbindungsvalidierung zu aktivieren bzw. zu inaktivieren.

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 11. Konfigurationsoptionen für das Repository.

Name	Beschreibung	Einstellungen
Grenze für kategoriale Werte	Begrenzt die Zahl der kategorialen Variablenwerte, die als IBM SPSS Modeler-Datenstrommetadaten gespeichert werden. Die gespeicherten Werte werden in den Inhalt aufgenommen, der bei der Durchführung von Suchvorgängen ausgewertet wird. Die Begrenzung ist nötig, um beim Speichern von Datenströmen im Repository und bei der Durchführung von Suchvorgängen Zeit 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 inaktivieren. Geben Sie 1 oder eine höhere Zahl ein, um die Zahl der gespeicherten Werte zu begrenzen.
Content-Repository-Endpunkt	Definiert die Web-Service-Endpunktadresse für das Repository.	URL.
Anmeldekennwörter müssen verschlüsselt sein	Anmeldekennwörter müssen verschlüsselt sein. "Falsch" gibt an, dass Kennwörter als unverschlüsselter Text übergeben werden dürfen. **Anmerkung:** Diese Option ist redundant für Bereitstellungen von IBM SPSS Collaboration and Deployment Services, bei denen SSL bereits aktiviert ist, und sollte nur bei Bereitstellungen ohne SSL verwendet werden, um Anmeldekennwörter zu verschlüsseln.	Standardmäßig inaktiviert.
Standardzeichensatz	Definiert das Standardzeichen für den Inhalt, der vom/ins Serverdateisystem heruntergeladen oder hochgeladen wird, oder für die Anzeige von Repository-Dateien in einem Web-Browser. 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.
Ressourcenübertragung disponieren	Gibt an, ob für Ressourcenübertragungsvorgänge zugeteilte Systemressourcen freigegeben werden sollen. Die Inaktivierung wird nicht empfohlen und darf nur zu Debugging-Zwecken verwendet werden.	Standardmäßig aktiviert.
Leistungsdaten protokollieren	"Wahr" gibt an, dass Leistungsdaten protokolliert werden.	Standardmäßig inaktiviert.
Nachrichtenbusbenachrichtigung aktiviert	Gibt an, ob der Repository-Server mit dem Nachrichtenbus verknüpft werden soll.	Standardmäßig aktiviert.

Tabelle 11. Konfigurationsoptionen für das Repository (Forts.).

Name	Beschreibung	Einstellungen
Kennwortanzeige für Modeler-Parameter	IBM SPSS Modeler-Datenstromparameter, die diese Zeichenfolge enthalten, werden beim Speichern verschlüsselt und in der Benutzerschnittstelle maskiert, wenn die Ausführung eines Datenstroms geplant wird.	Maskiertes Kennwort.
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 ist 15.
Größe des Thread-Pools neu indizieren	Definiert die Zahl der Threads, die für die Neuindizierung des Repositorys verwendet werden.	Ganzzahl. Der Standardwert ist 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) inaktiviert werden.	Standardmäßig aktiviert.
Wartungshäufigkeit für Repository	Legt die Häufigkeit (in Minuten) fest, mit der der Wartungsservice für das Repository ausgeführt werden soll. Der Repository-Service muss neu gestartet werden, damit die Änderungen wirksam werden.	Ganzzahl. Der Standardwert ist 60 Minuten.
Repository-Wartung – Master	Legt fest, ob der Wartungsservice für das Repository nur auf dem Masterknoten im Server-Cluster ausgeführt werden soll.	Wahr oder Falsch. Die Standardeinstellung lautet "Falsch".
Anfangsdatum für Repository-Wartung	Legt Datum und Uhrzeit für den Start des Wartungsservice für das Repository fest. Ungültige Datumsangaben oder Datumsangaben vor dem aktuellen Datum werden ignoriert und der Service wird sofort gestartet. Wenn die angegebene Uhrzeit für den Start in der Vergangenheit liegt, wird der Service 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 Wartungsservice fest.	Ganzzahl. Der Standardwert ist 30 Minuten.
Beginn der Repository-Wartung (Min.)	Legt die Mindestverzögerungszeit für den Start des Wartungsservice fest.	Ganzzahl. Der Standardwert ist 5 Minuten.

Tabelle 11. Konfigurationsoptionen für das Repository (Forts.).

Name	Beschreibung	Einstellungen
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) an und ermöglicht, dass der Wartungsservice 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 inaktiviert.
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 Seitenergebnis der Ressourcenübertragung	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 Benutzerschnittstelle angezeigt werden können. Die Größe des Ergebniscache 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 Speicherbelegung.	Ganzzahl. Der Standardwert ist 5.

Tabelle 11. Konfigurationsoptionen für das Repository (Forts.).

Name	Beschreibung	Einstellungen
Aktualisierung der Datenstromeigenschaften	Sofern verfügbar, gibt diese Option an, ob Datenstromeigenschaften aktualisiert werden, wenn die Datei im Repository veröffentlicht wird. Durch Inaktivieren dieser Option (empfohlen) lässt sich eventuell die Leistungsfähigkeit verbessern.	Standardmäßig aktiviert.
Ausführbare Serverprogramme validieren	Gibt an, ob ausführbare Serverdateien beim Speichern im Repository validiert werden sollen.	Standardmäßig aktiviert.
Versionsbegrenzung - maximale Anzahl Versionen pro Datei	Maximale Anzahl der Versionen, die für jede Datei gespeichert werden sollen. Wenn die Obergrenze erreicht ist, werden die ältesten Dateiversionen durch neue Versionen ersetzt.	Ganzzahl. Der Standardwert ist 10.
Versionsbegrenzung - nicht beschriftete Versionen entfernen	Nicht beschriftete Dateiversionen, die die maximale Anzahl der Versionen pro Datei überschreiten, werden automatisch entfernt.	Wahr oder Falsch. Die Standardeinstellung lautet "Falsch".
Versionsbegrenzung - nach Markierung sortieren	Gibt an, ob Dateiversionen nach Markierungen (Standardeinstellung) oder nach Erstellungsdatum sortiert werden.	Standardmäßig aktiviert.

Scoring-Service

Mit den Konfigurationsoptionen für den 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 12. Scoring-Service-Konfigurationsoptionen.

Name	Beschreibung	Einstellungen
Anwendungsserverauthentifizierung für WS-Security	Definiert, ob Anwendungsserver-JAAS-Authentifizierung für WS-Security verwendet werden soll.	Standardmäßig inaktiviert.
Auditzeitabstand	Die Zahl der Millisekunden zwischen Auditaktualisierungen.	Ganzzahl. Der Standardwert ist 3600000.
Standardprotokollziel	Standardprotokollziel.	Eine bereitstellungs- 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.
Metriken-Timer-Zeitraum	Die Zahl der Millisekunden zwischen Metrikaktualisierungen.	Ganzzahl. Der Standardwert ist 5000.

Tabelle 12. Scoring-Service-Konfigurationsoptionen (Forts.).

Name	Beschreibung	Einstellungen
Hostnamen auflösen	Definiert, ob der Scoring-Service versuchen soll, Hostnamen aufzulösen.	Standardmäßig aktiviert.
Arbeitspool - maximale Größe	Maximale Größe des Worker-Pools.	Ganzzahl. Der Standardwert ist 100.

Suchen

Die Konfigurationsoption für Suchen ermöglicht es Ihnen, die Anzahl der Treffer, die auf einer Suchergebnisseite in IBM SPSS Deployment Manager angezeigt werden sollen, und die Größe des Ergebnissets anzugeben sowie festzulegen, ob Suchen in Auditansichten 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 13. Konfigurationsoptionen für die Suche.

Name	Beschreibung	Einstellungen
Suchvorgang-Audit	Protokolliert jede Suche in der Auditansicht. Weitere Informationen finden Sie im Thema Kapitel 15, „Auditing des Repositorys", auf Seite 89. Beachten Sie, dass die Suchfunktion durch das Aktivieren dieser Option verlangsamt werden kann.	Standardmäßig inaktiviert.
Standard-Seitengröße	Anzahl der Suchergebnisse, die auf einer Seite angezeigt werden.	Ganzzahl. Der Standardwert ist 25.
Zeilen maximal	Maximale Anzahl an Zeilen in einem Suchergebnisset. 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 Ergebnissets zu beschränken und Probleme aufgrund von Speicherknappheit und Client-Timeouts zu vermeiden).	Ganzzahl. Der Standardwert ist -1.
Suchservicewartung aktiviert	Gibt an, ob Wartungsaktivitäten für den Suchservice aktiviert sind.	Standardmäßig aktiviert.

Sicherheit

Die Konfigurationsoptionen für die Sicherheit 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 14. Konfigurationsoptionen für die Sicherheit.

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. Der Standardwert ist 30. Der Wert 0 bedeutet, dass Benutzersperren niemals automatisch aufgehoben werden.
Anmeldungen im Cache ablegen	Speichert Anmeldungen für schnellere Reaktion von Web-Services. Wenn aktiviert, werden Änderungen an Benutzern, Gruppen oder Rollen erst nach 30 Minuten oder später wirksam. Erfordert einen Serverneustart.	Standardmäßig aktiviert.
Cachesitzungs-Zeitlimitüberschreitung	Anzahl der Minuten, bevor die Sicherheitssitzung eines inaktiven Benutzers entfernt wird. **Anmerkung:** Diese Einstellung wirkt sich nur auf Sitzungen der browserbasierten Instanz von IBM SPSS Deployment Manager aus.	Ganzzahl. Der Standardwert ist 30.
Gruppen mit Einschränkung für Berechtigungsnachweise	Gruppen, die Berechtigungsnachweise in IBM SPSS Deployment Manager oder SPSS Modeler nicht anzeigen können. Beispiel: In Ihrem Unternehmen gibt es Benutzer, die Analysejobs und -datenströme ausführen. Sie möchten aber nicht, dass diese Benutzer direkten Zugriff auf Datenquellen haben.	Wenn Sie mehrere Gruppen definieren, geben Sie jede Gruppe in einer separaten Zeile ein.
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. Der Standardwert ist 5.
Clients inaktivieren	Inaktiviert die Anmeldung für Clientanwendungen von IBM SPSS Collaboration and Deployment Services (IBM SPSS Deployment Manager, IBM SPSS Collaboration and Deployment Services Deployment Portal usw.)	Standardmäßig inaktiviert.
Kennwort verschlüsseln	Macht die Verwendung verschlüsselter Kennwörter für Web-Services erforderlich. Web-Services senden beim Anfordern von Kennwörtern einen Verschlüsselungsschlüssel. Der Server verschlüsselt das Kennwort mithilfe des bereitgestellten öffentlichen Schlüssels. Wenn **Kennwort verschlüsseln** aktiviert ist, dürfen Web-Services keine Kennwörter anfordern, ohne einen Verschlüsselungsschlüssel zu liefern. Dies betrifft Benutzervorgaben, Content-Repository-Berechtigungsnachweise und ähnliche Services.	Standardmäßig aktiviert.

Tabelle 14. Konfigurationsoptionen für die Sicherheit (Forts.).

Name	Beschreibung	Einstellungen
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 inaktiviert werden, wenn bei einem fernen Benutzerverzeichnis die Groß-/Kleinschreibung der Benutzer-IDs beachtet werden muss.	Standardmäßig aktiviert.
Nachricht	Die Nachricht, die auf Eingangsanzeige der browserbasierten Instanz von IBM SPSS Deployment Manager angezeigt wird.	Nachrichtentext. 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 inaktiviert.
Hostnamen auflösen	Legt fest, ob Web-Service-Aufrufe versuchen sollen, Hostnamen aufzulösen.	Standardmäßig aktiviert.

Setup

Mit der Konfigurationsoption für das Setup können Sie verschiedene Setup-Einstellungen für das Repository festlegen, beispielsweise das auf IBM SPSS Collaboration and Deployment Services verweisende URL-Präfix, JMS-Warteschlangeneinstellungen und JMS-Nachrichtenbus-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 15. Konfigurationsoptionen für das Setup.

Name	Beschreibung	Einstellungen
Log-JMS Connection Factory	JNDI-Name der Log-JMS Connection Factory.	Eine bereitstellungs- 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 bereitstellungs- oder serverspezifische Zeichenfolge, bei der Groß- und Kleinschreibung beachtet wird und die vom JNDI-Service verwendet wird, um die Log-JMS-Warteschlange zu kennzeichnen.

Tabelle 15. Konfigurationsoptionen für das Setup (Forts.).

Name	Beschreibung	Einstellungen
Nachrichtenbus-JMS Connection Factory	JNDI-Name der Nachrichtenbus-JMS Connection Factory.	Eine bereitstellungs- oder serverspezifische Zeichenfolge, bei der zwischen Groß- und Kleinschreibung unterschieden wird und die vom JNDI-Service verwendet wird, um die Nachrichtenbus-JMS Connection Factory zu kennzeichnen.
Nachrichtenbus-JMS-Topic	JNDI-Name des Nachrichtenbus-JMS-Topics.	Eine bereitstellungs- oder serverspezifische Zeichenfolge, bei der zwischen Groß- und Kleinschreibung unterschieden wird und die vom JNDI-Service verwendet wird, um das Nachrichtenbus-JMS-Topic 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 neu gestartet werden, damit Änderungen am Präfix wirksam werden.	URL. **Einschränkung:** Beenden Sie die URL-Angabe nicht mit einem Schrägstrich. Beispielsweise müssen Sie `http://server:8080/root` statt `http://server:8080/root/` angeben.

CMOR

Die Konfigurationsoption für CMOR 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 Benutzerschnittstelle ausgeblendet und ein Zugriff darauf sollte nur erforderlich sein, wenn die Zeichenbeschränkung aufgrund von Fehlern erhöht werden muss. Wenn die Anzahl der in Versionsbeschriftungen verwendeten Zeichen die angegebene Obergrenze überschreitet, kann das System die verfügbare Liste nur abrufen, wenn ein Datenprovider für eine Scoring-Konfiguration ausgewählt wird, und das Serverprotokoll enthält Kürzungsfehler. Wenn die Anzahl der Beschriftungen nicht verringert werden kann, muss die Zeichenbeschränkung für UDF auf einen höheren Wert gesetzt werden. So ändern Sie die Beschränkung:

1. Klicken Sie auf der Seite "Konfiguration" auf den Link **Konfiguration**, um die ausgeblendeten Einstellungen anzuzeigen.
2. Klicken Sie in der Einstellungsliste unter "CMOR" auf **Zeichenbeschränkung für UDF**. Die aktuelle Obergrenze für die Anzahl der Zeichen wird angezeigt.
3. Ändern Sie den Wert nach Bedarf.
4. Klicken Sie auf **Festlegen**, um den neuen Wert festzulegen.
5. Melden Sie sich ab und starten Sie den Repository-Server erneut.

   Bei einigen Datenbanken, wie SQL Server oder Db2, 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:
6. Stoppen Sie den Server nach der Änderung des Konfigurationswerts.

7. 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.
8. 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 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)`

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 Seite **MIME-Typen und Dateitypsymboler** von IBM SPSS Deployment Manager, auf die Sie durch Klicken auf **MIME-Typen** in der Navigationsliste zugreifen können.

Auf der Seite **MIME-Typen und Dateitypsymbole** 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.

Anmerkung: Viele gängige 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. Weitere Informationen finden Sie im Thema „Hinzufügen von MIME-Typzuordnungen".

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 gibt das Format der Medien an 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 Herstelleruntertyp 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.

So fügen eine neue MIME-Typzuordnung hinzu:

1. Klicken Sie auf der Seite **MIME-Typen und Dateitypsymbole** auf **Neuen MIME-Typ hinzufügen**. Die Seite **MIME-Typen und Dateitypsymbole hinzufügen** wird angezeigt.
2. 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*.

3. Geben Sie den hinzuzufügenden MIME-Typ ein.
4. Geben Sie die Dateiendungen ein, die mit dem MIME-Typ verbunden werden sollen. Setzen Sie zwischen Einträgen ein Leerzeichen, wenn Sie mehrere Dateiendungen angeben.
5. 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** aus.
6. Klicken Sie auf **Speichern**, um den MIME-Typ hinzuzufügen und zur Seite **MIME-Typen und Dateitypsymbole hinzufügen** zurückzukehren, oder auf **Abbrechen**, um zurückzukehren, ohne den MIME-Typ auf dem Server zu speichern.

Bearbeiten von MIME-Typzuordnungen

So bearbeiten Sie einen vorhandenen MIME-Typ:

1. Klicken Sie auf der Seite **MIME-Typen und Dateitypsymbole** auf den Namen des MIME-Typs, der bearbeitet werden soll. Die Seite **MIME-Typen und Dateitypsymbole bearbeiten** für diesen MIME-Typ wird angezeigt.
2. Ändern Sie die Einstellungen wie erforderlich. Symbole werden nur geändert, wenn Sie eine neue Datei oder **Nein** auswählen. Wählen Sie **Nein** zum Löschen eines Symbols aus.
3. Klicken Sie auf **Speichern**, um die neuen Einstellungen für den MIME-Typ zu speichern und zur Seite **MIME-Typen und Dateitypsymbole hinzufügen** zu gelangen, oder auf **Abbrechen**, um zurückzukehren, ohne die MIME-Typ-Einstellungen auf dem Server zu speichern.

Löschen von MIME-Typzuordnungen

So löschen Sie einen vorhandenen MIME-Typ:

- Klicken Sie auf der Seite **MIME-Typen und Dateitypsymbole** auf das Symbol **Löschen** des MIME-Typs, der gelöscht werden soll. Die MIME-Typentabelle wird aktualisiert; der gelöschte MIME-Typ ist nicht mehr enthalten.

Kapitel 11. Neuindizierung des Repositorys

Die Indizierung wird verwendet, um die die Suche von IBM SPSS Collaboration and Deployment Services Repository 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 Jobausgabe, beim Start erzwungen wird. Weitere Informationen finden Sie im Thema „Prozessmanagement" auf Seite 50. Die Repository-Suche wird automatisch inaktiviert, während die Neuinidizierung beim Start läuft.

Eine Neuinidizierung kann auch in der browserbasierten Instanz von IBM SPSS Deployment Manager auf Anforderung eines autorisierten Benutzers durchgeführt werden. Weitere Informationen finden Sie im Thema „Aktionen" auf Seite 25.

Anmerkung: Die Neuindizierung ist ein ressourcenintensiver und langwieriger Prozess, der nur ausgeführt werden sollte, wenn es unbedingt erforderlich ist, beispielsweise 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 inaktiviert werden. Es ist jedoch nicht ratsam, den Index zu löschen, während das System verwendet wird.

So indizieren Sie das Repository neu:

1. Klicken Sie in der browserbasierten Instanz von IBM SPSS Deployment Manager in der Navigationsliste auf **Repository-Index**. Die Seite "Indizierung des Content-Repository" wird geöffnet.
2. Führen Sie eine der folgenden Aktionen aus:
   - Wenn keine Benutzer beim Repository angemeldet sind, wählen Sie **Gesamten Index vor Neuindizierung löschen** aus.
   - Wenn noch Benutzer beim Repository angemeldet sind, wählen Sie **Clients während Indizierung inaktivieren** aus.
3. Klicken Sie auf **Indizierung starten**. Während der Index neu erstellt wird, zeigt die Seite "Indizierungsstatus des Content-Repository" die Statistik der verarbeiteten Objekte.

Kapitel 12. Repository-Wartung

Zur Wartung von IBM SPSS Collaboration and Deployment Services Repository 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 von 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 Zeitlimitüberschreitung fehlschlagen. Um derartige Probleme zu vermeiden, sollten regelmäßig unnötige Objekte und Versionen entfernt werden.

Kandidaten für eine Entfernung sind folgende Elemente:

- Nicht beschriftete Versionen von Objekten, die nicht benötigt werden
- Unnötige Jobartefakte
- Abgelaufene übergebene Arbeiten Weitere Informationen finden Sie im Thema „Entfernen abgelaufener übergebener Arbeiten" auf Seite 69.
- Alte Jobverläufe Weitere Informationen finden Sie im Thema „Verwalten der Größe des Jobverlaufs" auf Seite 69.

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 Stapelvorgang 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 Wartungsservice verwaltet.

Repository-Sicherung

Die Daten und die Anwendungseinstellungen von IBM SPSS Collaboration and Deployment Services Repository 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 Wartungsservice

Beim Löschen von Elementen steht das Element mit sofortiger Wirkung für keinen Client von IBM SPSS Collaboration and Deployment Services Repository mehr zur Verfügung. Das Element wird zu diesem Zeitpunkt jedoch nicht entfernt, sondern lediglich für die Löschung gekennzeichnet. Die eigentliche Löschung wird durch einen Wartungsservice durchgeführt. Dieser Service 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 Service im System. Der Wartungsservice 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 der Beschriftung *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 Wartungsservice führt eine Reihe von Aufgaben durch, unter anderem:

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

Der Service wird gemäß einem Zeitplan ausgeführt, der durch eine Reihe von Konfigurationsparametern definiert wird. Werte für diese Parameter können Sie über die browserbasierte Instanz von IBM SPSS 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 Wartungsservice 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 Wartungsservice gestartet werden sollte. Wenn der Service zum festgelegten Zeitpunkt nicht gestartet werden kann, ist dieser Wert die maximale Zeitdauer, während derer versucht wird, den Service 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 Wartungsservice gestartet werden sollte. Wenn der Service zum festgelegten Zeitpunkt nicht gestartet werden kann, ist dieser Wert die minimale Zeitdauer, während derer versucht wird, den Service 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 Wartungsservice angibt. Beispielsweise wird beim Wert 90 der Service 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 Wartungsservice 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 Server für IBM SPSS Collaboration and Deployment Services in einer Clusterumgebung ausgeführt wird, haben Sie die Wahl, ob der Wartungsservice auf allen Clusterknoten oder nur auf dem Masterknoten ausgeführt werden soll. Wählen Sie in der Konfigurationsliste die Option **Repository-Wartung – Master** aus. Durch Auswahl dieser Option wird der Service auf den Masterknoten beschränkt. Klicken Sie auf **Setzen**.
8. Führen Sie einen Neustart des Servers für IBM SPSS Collaboration and Deployment Services durch, um mit der Verwendung der neuen Einstellungen zu beginnen.

Weitere Informationen zu diesen Konfigurationseinstellungen finden Sie unter „Repository” auf Seite 52.

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 Wartungsservice werden die Elemente aus dem Repository entfernt.

Sie können diese Funktion auf der Seite "Konfiguration" in der browserbasierten Instanz von IBM SPSS 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” auf Seite 50.

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 Wartungsservice 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" in der browserbasierten Instanz von IBM SPSS 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” auf Seite 50.

Überwachen von Wartungsaktivitäten

Zusammenfassungen über die Aktivitäten des Wartungsservice können in die Systemprotokolldateien aufgenommen werden. Dadurch können Sie ermitteln, welche Aufgaben bei der Aktivierung des Service durchgeführt werden.

So aktivieren Sie die Protokollierung für den Wartungsservice:

1. Öffnen Sie die Konfigurationsdatei für die Protokollierung in einem Texteditor.

   Der Speicherort der Konfigurationsdatei für die Protokollierung für IBM SPSS Collaboration and Deployment Services Repository variiert abhängig vom Hostanwendungsserver.

   - **WebSphere:** `<Repository-Installationsverzeichnis>/platform/log4j.properties`
   - **Liberty:** `<Repository-Installationsverzeichnis>/platform/log4j.properties`
   - **JBoss:** `<JBoss-Serververzeichnis>/deploy/jboss-logging.xml`

2. Fügen Sie der Protokollfunktion *com.spss.process.internal.maintenance* einen Eintrag hinzu und setzen Sie die Protokollierungsebene auf *DEBUG*. Fügen Sie in der Datei `log4j.properties` die folgende Zeile hinzu:

   ```
   log4j.logger.com.spss.process.internal.maintenance=DEBUG, R
   ```

   Informationen zum Hinzufügen von Protokollfunktionen zur JBoss-Konfigurationsdatei für die Protokollierung finden Sie in der JBoss-Dokumentation.

3. Speichern Sie Ihre Änderungen.
4. Starten Sie den Repository-Server erneut.

Bei der Aktivierung des Wartungsservice wird folgende Nachricht zur Protokollausgabe hinzugefügt:

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

Weitere Informationen zu den Protokollierungsservices finden Sie in der Installations- und Konfigurationsdokumentation zum Repository-Server.

Begrenzen der Anzahl der Dateiversionen

Die maximale Anzahl der Dateiversionen kann automatisiert und gesteuert werden. Sie können Ihr System so konfigurieren, dass die ältesten Dateiversionen automatisch gelöscht werden, wenn die Anzahl der Versionen einen angegebenen Grenzwert erreicht. Wenn der Wartungsservice aktiviert wird, werden die ältesten Dateiversionen aus dem Repository entfernt.

Ältere Dateiversionen werden in beinahe allen Fällen nicht verwendet, belegen Speicherplatz und verringern die Systemleistung. Das Bereinigungsdienstprogramm untersucht das Repository regelmäßig (standardmäßig jede Stunde) und prüft auf Dateiversionen, die den definierten Grenzwert überschreiten.

Sie können diese Features über die Seite **Konfiguration** steuern, die in der browserbasierten Instanz von IBM SPSS Deployment Manager zur Verfügung steht.

Anmerkung: Es werden nur nicht beschriftete Dateiversionen gelöscht. Beschriftete Versionen sind nicht betroffen.

Führen Sie die folgenden Schritte aus, um die Dateiversionen automatisch zu verwalten:

1. Wählen Sie **Versionsbegrenzung - nicht beschriftete Versionen entfernen** aus der Repository-Gruppe aus. Wenn diese Einstellung ausgewählt ist, werden nicht beschriftete Versionen, die die maximale Anzahl der Versionen pro Datei übersteigen, automatisch entfernt. Standardmäßig ist die Einstellung nicht aktiviert. Wenn Sie die Einstellung ausgewählt bzw. ihre Auswahl aufgehoben haben, klicken Sie auf **Festlegen**.
2. Geben Sie die maximale Anzahl der Dateiversionen in **Versionsbegrenzung - maximale Anzahl Versionen pro Datei** in der Repository-Gruppe ein. Die Einstellung gibt die maximale Anzahl der Versionen an, die für jede Datei gespeichert werden sollen (der Standardwert ist 10). Wenn Sie die maximale Anzahl der Dateiversionen eingegeben haben, klicken Sie auf **Festlegen**.

   Anmerkung: Wenn dieser Wert kleiner als der Wert für **Obergrenze für Jobverlauf** ist, enthalten die Jobverlaufsdatensätze möglicherweise keine Artefakte.

3. Die Einstellung **Versionsbegrenzung - nach Markierung sortieren** in der Repository-Gruppe legt fest, ob die Dateiversionen nach Markierungen (Standardeinstellung) oder nach Erstellungsdatum sortiert werden.

Weitere Informationen zu diesen Konfigurationseinstellungen finden Sie unter „Repository" auf Seite 52.

Stapellöschung

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 Bereinigungsdienstprogramm 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 einer Beschriftung
- Anzahl der Versionen
- Erstellungsdatum

Beispielsweise können Sie mit dem Bereinigungsdienstprogramm bei jeder IBM SPSS Statistics-Syntaxdatei in einem bestimmten Ordner alle Versionen bis auf die letzten drei löschen. Oder Sie können alle Versionen ohne Beschriftung, die älter sind als ein bestimmtes Datum, aus IBM SPSS Modeler-Datenströmen löschen.

Wenn das automatische Wartungsframework aktiviert ist, werden die ausgewählten Elemente für eine anschließende Löschung bei der nächsten verfügbaren Gelegenheit gekennzeichnet. Wenn das Wartungsframework inaktiviert ist, werden die Elemente sofort gelöscht.

Das Bereinigungsdienstprogramm ist komplett Java-basiert und kann auf jeder von IBM SPSS Collaboration and Deployment Services unterstützten 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 Bereinigungsdienstprogramm über die Befehlszeile ausführen oder Jobschritte 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 Bereinigungsdienstprogramm verarbeitet werden.

Ausführen des Bereinigungsdienstprogramms

Der Befehl zur Ausführung des Bereinigungsdienstprogramms weist folgende Struktur auf:

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

Auf den Befehl `cleanup` folgt eine durch Leerzeichen getrennte Liste mit Parametern und zugehörigen Werten, die den Löschvorgang definieren. Die einzelnen Parameterangaben enthalten den Parameternamen, ein Gleichheitszeichen sowie den Parameterwert. In der Tabelle Tabelle 17 sind die einzelnen Parameter beschrieben.

Tabelle 17. Parameter des Bereinigungsdienstprogramms.

Parameter	Verwendung	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 zu 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 Kennwort 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.
`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 Beschriftungen gelöscht werden sollen oder nicht. Die Standardeinstellung ist "falsch".
`versionsToKeep`	Optional	Die Anzahl der aktuellsten Versionen, die beibehalten werden sollen. Der Standardwert ist 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 Bereinigungsdienstprogramm 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 Bereinigungsdienstprogramm kann mit folgenden Schritten aufgerufen werden:

1. Prüfen Sie, ob die Umgebungsvariable *Path* Ihren Java-Pfad enthält.
2. Navigieren Sie an einer Eingabeaufforderung zu dem Verzeichnis, das das Bereinigungsdienstprogramm 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 Beschriftung zum Löschen ausgewählt. Der Parameter `testMode` verhindert, dass Versionen tatsächlich gelöscht werden, sodass Sie die Datei *cleanup.log* prüfen können, um die ausgewählten Versionen zu ermitteln, 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 Stapellöschung

Mithilfe eines allgemeinen Jobschritts können Sie die Stapellöschung über einen Job von IBM SPSS Collaboration and Deployment Services initiieren.

Gehen Sie wie folgt vor, um einen Jobschritt für die Stapellöschung in IBM SPSS Deployment Manager zu erstellen:

1. Fügen Sie einen allgemeinen Jobschritt zu einem Job hinzu.
2. Klicken Sie auf den Jobschritt, 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 Bereinigungsdienstprogramm für Ihr System ein, gefolgt von Parametern für das Bereinigungsdienstprogramm, in dem die Löschaufgabe definiert wird.
4. Wenn die Löschaufgabe den Parameter `logfile` einschließt und das Protokoll in IBM SPSS Collaboration and Deployment Services Repository gespeichert werden soll, verwenden Sie die Registerkarte "Ausgabedateien" zur Angabe der Zielposition für die Datei.
5. Speichern Sie den Job.

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 Dokumentation zu IBM SPSS Deployment Manager.

Kapitel 13. Benachrichtigungen

IBM SPSS Collaboration and Deployment Services bietet die Mechanismen von *Benachrichtigungen* und *Abonnements*, um die Benutzer über Änderungen an Objekten von IBM SPSS Collaboration and Deployment Services Repository sowie Jobverarbeitungsergebnisse auf dem Laufenden zu halten. Sowohl Benachrichtigungen als auch Abonnements erzeugen E-Mail-Nachrichten, 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 enthalten sind, befinden sich in den Unterverzeichnissen von *<Installationsverzeichnis>\components\notification\templates*. Die Namen der Unterverzeichnisse entsprechen dem allgemeinen Ereignistyp. Beispielsweise enthält der Ordner *components\notification\templates\PRMS\Completioncomponents\notification\templates\PRMS\Completion* zwei Nachrichtenvorlagen. Diese Vorlagen, *job_success.xsl* und *job_failure.xsl*, entsprechen der erfolgreichen (Success) und fehlgeschlagenen (Failure) Jobausführung. Wenn ein Job erfolgreich abgeschlossen wird, verwendet IBM SPSS Collaboration and Deployment Services die Vorlage *job_success*, um eine Hinweisnachricht zu generieren, die die erfolgreiche Ausführung mitteilt. Inhalt und Erscheinungsbild der Hinweisnachrichten können durch Ändern der Vorlagen angepasst werden.

Struktur von Benachrichtigungsvorlagen

Struktur von Hinweisnachrichtenvorlagen

Benachrichtigungsvorlagen transformieren Ereignisdaten in Hinweisnachrichten und verwenden dafür die Sprach der *Velocity*-Vorlage von Apache.

Struktur von Velocity-Vorlagen

Eine Velocity-Vorlage hat die Dateiendung `*.vm`. Die Vorlage generiert eine Nachricht 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=Jobfertigstellung
/mimeMessage/messageContent[text/plain;charset=utf-8]=Der Job wurde erfolgreich abgeschlossen.
```

Weitere Informationen zu Velocity finden Sie in der Dokumentation zu Apache Velocity Project.

Nachrichteneigenschaften

E-Mail-Benachrichtigungsvorlagen können Eigenschaften enthalten, die festlegen, wie eine Nachricht 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. Wenn Sun JVM bei der Repository-Installation verwendet wird, entsprechen die SMTP-Eigenschaften den in der folgenden Tabelle definierten Eigenschaften der JavaMail-API für die Nachrichtenbehandlung. 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 18. Nachrichteneigenschaften.

Nachrichteneigenschaft	Attribut	Ereigniseigenschaft	Beschreibung
mail.debug	Wert	MailSmtpDebug	Ein boolescher Wert, der den anfänglichen Debugmodus angibt. Der Standardwert lautet "false".
mail.smtp.user	Wert	MailSmtpUser	Der Standard-SMTP-Benutzername.
mail.smtp.password	Wert	MailSmtpPassword	Das SMTP-Benutzerkennwort.
mail.smtp.host	Wert	MailSmtpHost	Der SMTP-Server, zu 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 ist 25.
mail.smtp.connectiontimeout	Wert	MailSmtpConnectionTimeout	Das Zeitlimit für die Socketverbindung in Millisekunden. Standardmäßig ist das Zeitlimit unendlich.
	Wert	MailSmtpTimeout	Das Zeitlimit für Socket-E/A in Millisekunden. Standardmäßig ist das Zeitlimit unendlich.
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	Beschriftung	MailSmtpFromPersonal	Die Beschriftung für die Adresse des Absenders
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 boolescher 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 boolescher Wert, der angibt, ob der Benutzer über den `AUTH`-Befehl authentifiziert werden soll oder nicht. Der Standardwert lautet "false".

Tabelle 18. Nachrichteneigenschaften (Forts.).

Nachrichteneigenschaft	Attribut	Ereigniseigenschaft	Beschreibung
mail.smtp.dsn.notify	Wert	MailSmtpDsnNotify	Gibt die Umstände an, unter denen der SMTP-Server Benachrichtigungen über den Zustellungsstatus an den Absender der Nachricht 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 Nachricht 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 Beschriftungsargumente in eckigen Klammern stehen müssen, wie im folgenden Beispiel angegeben:

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

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

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

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

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

Nachrichteninhalt

Der Inhalt einer Hinweisnachricht 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. Beispielsweise fügt `Jobschritt ${JobName}/${JobStepName} schlug fehl um ${JobStepEnd}` den Text mit den aktuellen Werten für die Eigenschaften *JobName*, *JobStepName* und *JobStepEnd* ein.

Die Variablen, die in eine Nachricht 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*, eine Zeitmarke, die die Beginnzeit des Jobs angibt.
- *JobEnd*, eine Zeitmarke, die die Endzeit des Jobs angibt.
- *JobSuccess*, ein boolescher Wert, der anzeigt, ob der Job erfolgreich war oder nicht.
- *JobStatusURL*, eine Zeichenfolge, die die URL angibt, über die der Jobstatus aufgerufen werden kann.

- *JobStepName*, eine Zeichenfolge, die den Namen des Jobs angibt.
- *JobStepEnd*, eine Zeitmarke, die die Endzeit des Jobs angibt.
- *JobStepArtifacts*, ein Array von Zeichenfolgenwerten, das die URLs der Ausgabedateien für Jobschritte angibt.
- *JobStepStatusURL*, eine Zeichenfolge, die die URL angibt, über die der Jobschrittstatus 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 die HTTP-URL angibt, unter der 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 Velocity-Beispielvorlage für Benachrichtigungen beim Erfolg von Jobschritten werden die Namen des Jobs und des Jobschritts in die Betreffzeile eingefügt. Der Inhalt der Nachricht enthält außerdem die Endzeiten für den Schritt, die URL, über die 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 um ${JobStart} gestartet und #if($JobSuccess) wurde erfolgreich ausgeführt
#else ist fehlgeschlagen um #end ${JobEnd}.

<p>Um das Jobprotokoll zu prüfen, wechseln Sie zu <a href='${JobStatusURL}'>${JobStatusURL}</a>.</p>.

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

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

Ursprüngliche Vorlage:

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

Nachrichtenformat

Eine Benachrichtigungsvorlage muss den MIME-Typ des Nachrichteninhalts 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*. Hinweisnachrichten werden als einfacher Text angezeigt. Dies ist die Standardeinstellung.
- *text/html*. Hinweisnachrichten enthalten HTML-Tags. Verwenden Sie diese Einstellung, um das Erscheinungsbild des Inhalts in der Nachricht zu beeinflussen. Die HTML-Tags in der Nachricht müssen einwandfrei gebildet werden.

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

HTML-Benachrichtigungsvorlagen können die Funktionen nutzen, die im Markup zulässig sind. Zum Beispiel kann die Nachricht einen Link auf eine Webseite oder zu einer Jobausgabe enthalten.

Folgende Vorlage generiert eine Hinweisnachricht 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 Jobausgabe.

```
/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">Dies ist eine maschinell erzeugte Nachricht.
            Bitte antworten Sie nicht darauf. 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>
```

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 Vorlagenset.
2. Ändern Sie den Wert, der `/mimeMessage/messageSubject` zugeordnet ist. Verwenden Sie die $-Notation, um Ereigniseigenschaftsvariablen in das Benachrichtigungsthema einzufügen. Weitere Informationen finden Sie im Thema „Nachrichteninhalt" auf Seite 77.
3. Definieren Sie den MIME-Typ der Nachricht. Der Wert des MIME-Typs wird in den eckigen Klammern hinter `messageContent` angegeben. Verwenden Sie für eine Standardtextnachricht den Wert *text/plain*. Verwenden Sie für eine HTML-Nachricht den Wert *text/html*. Weitere Informationen finden Sie im Thema „Nachrichtenformat" auf Seite 79.
4. Ändern Sie den Wert, der `messageContent` zugeordnet ist. Verwenden Sie die $-Notation, um Ereigniseigenschaftsvariablen in den Inhalt der Nachricht einzufügen.
5. Speichern Sie die Vorlage unter Verwendung ihres ursprünglichen Namens.

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

Jobstatus

Eine Benachrichtigungsvorlage, die die Eigenschaft *JobStatusURL* enthält, ergibt eine Nachricht mit einem Link zu Jobausgabe und -protokoll.

So zeigen Sie die Ergebnisse eines Jobs an:

1. Klicken Sie auf den Statuslink in der Hinweisnachricht. Die Anmeldungsseite für den Server wird geöffnet.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Klicken Sie auf **Anmelden**. Die Seite "Jobstatus" wird geöffnet.

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.

Name. Der Repository-Pfad des Jobs.

Version. Die Versionsbeschriftung 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**.
- Um die Details für den Jobschritt zu erweitern, die das Jobschrittprotokoll und alle resultierenden Ausgaben enthalten, klicken Sie auf das **+** neben dem Jobschrittnamen.

Die folgenden Informationen werden für einen Jobschritt bereitgestellt:

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 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**.

Jobstatus

Eine Benachrichtigungsvorlage, die die Eigenschaft *JobStatusURL* enthält, ergibt eine Nachricht mit einem Link zu Jobausgabe und -protokoll.

So zeigen Sie die Ergebnisse eines Jobs an:

1. Klicken Sie auf den Statuslink in der Hinweisnachricht. Die Anmeldungsseite für den Server wird geöffnet.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Klicken Sie auf **Anmelden**. Die Seite "Jobstatus" wird geöffnet.

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.

Name. Der Repository-Pfad des Jobs.

Version. Die Versionsbeschriftung 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**.
- Um die Details für den Jobschritt zu erweitern, die das Jobschrittprotokoll und alle resultierenden Ausgaben enthalten, klicken Sie auf das **+** neben dem Jobschrittnamen.

  Die folgenden Informationen werden für einen Jobschritt bereitgestellt:

  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 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**.

Optimieren der Leistung des Benachrichtigungsservice

Die Gesamtleistung des Benachrichtigungsservice ist eine Kombination aus der Leistung der Komponenten von IBM SPSS Collaboration and Deployment Services, 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 Benachrichtigungsservice zu befolgen.

Konfiguration des Benachrichtigungsservice

Konfigurationsoptionen für Benachrichtigungen

Die Leistung des Benachrichtigungsservice 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 es dem System, Benachrichtigungsereignisse zu ignorieren, für die keine entsprechenden Abonnements oder verknüpfte Benachrichtigungsprovider 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 gegebenenfalls die zusätzliche Vergrößerung des Cache (Konfigurationsoption *Ereignisfiltercache*) kann die Leistung des Benachrichtigungsservice verbessern. Vom Inaktivieren 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, z. B. einige Dutzend oder in wenigen Fällen mehrere Hundert. Vergrößern des Cache (Konfigurationsoption *Abonnement-ID-Cache*) kann die Leistung verbessern.
- Die persistente Ereigniswarteschlange ermöglicht es 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 Festschreibungsstapelgröße 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 Festschreibungsstapelgröße (Konfigurationsoption *Größe der persistenten Ereigniswarteschlange*) die Leistung verbessern, jedoch werden wegen der zusätzlichen Speicheranforderungen nur moderate Erhöhungen der Stapelgröße 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 Inaktivieren von binären Inhalten (E-Mail-Anhänge), die mit der Hinweisnachricht gesendet werden, kann die Leistung signifikant verbessert werden (Konfigurationsoption *Binärer Inhalt aktiviert*).

Das Generieren der Hinweisnachrichten mit binären Anhängen kann ein verarbeitungsintensiver Vorgang sein. Der Inhalt des binären Anhangs muss aus dem Repository gelesen, an die Hinweisnachricht angehängt und durch den geeigneten Verteilungskanal, z. B. einen E-Mail-Server, geleitet werden. Auch kann eine Transformation des binären Inhalts des Anhangs für bestimmte Arten von Hinweisnachrichten erforderlich sein. Beispielsweise vergrößern binäre Anhänge mit Base64-Codierung (SMTP) die Gesamtgröße der generierten Nachrichten um etwa 33 %. Die Systembelastung kann sogar noch umfangreicher werden, wenn eine Reihe von verschiedenen benutzerdefinierten Vorlagen zur Formatierung von Hinweisnachrichten mit umfangreichen Anhängen verwendet wird. In diesen Fällen muss der Benachrichtigungsservice Nachrichten formatieren, Anhänge hinzufügen und jede Nachricht separat durch den Verteilungskanal "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 Hinweisnachrichten mit Anlagen zu begrenzen.

- Die Verarbeitung und Verteilung von Hinweisnachrichten 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 Seite 45.

Dedizierter SMTP-Server

Die Leistung des Zustellungskanals, z. B. eines E-Mail-Servers, ist der entscheidende Faktor bei der Steuerung der Gesamtleistung des Benachrichtigungsservice. Für Benachrichtigungen von IBM SPSS Collaboration and Deployment Services 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 Hinweisnachricht in die Mailer-Warteschlange erheblich verkürzt und damit die Leistung des Benachrichtigungsservice 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 Benachrichtigungsservice zur Kommunikation mit dem E-Mail-Server über das Netz 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 Verarbeitungsthreads im Ereignissammlungspool des Benachrichtigungsservice von IBM SPSS Collaboration and Deployment Services sein. Wenn die Anzahl an Threads auf dem Distributionsserver nicht ausreicht, kann der Benachrichtigungsservice nicht effizient mit diesem kommunizieren.

Allgemeine Empfehlungen

Mithilfe der folgenden Techniken lässt sich die Leistung des Benachrichtigungsservice deutlich verbessern, ohne die verfügbare Gesamtfunktionalität von IBM SPSS Collaboration and Deployment Services 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 Unternehmensverzeichnisservern (Microsoft Exchange, Lotus Domino usw.) geführt werden. Mit dieser Methode werden ziemlich viele Datenbankabfragen vermieden, die der Benachrichtigungsservice ausführen muss, um Empfänger und ihre Zustellgeräte abzurufen. Spezialisierte SMTP-Unternehmensserver sollten in der Lage sein, verfügbare Ressourcen zu verwenden und die Zustellung der Hinweisnachrichten 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 Hinweisnachrichten für einen bestimmten Ereignistyp dienen. Jedoch reicht es unter normalen Umständen aus, Hinweisnachrichten 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. Weitere Informationen finden Sie im Thema „Bearbeiten von Benachrichtigungsvorlagen" auf Seite 80. Eine große Anzahl benutzerdefinierter 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 Hinweisnachricht separat formatiert werden muss. Dasselbe Prinzip gilt für eine benutzerdefinierte SMTP-Absenderadresse. In den meisten Fällen genügt eine einzelne Standardsenderadresse, die als Repository-Konfigurationsoption angegeben ist. Selbst wenn der Inhalt (Betreff und Text) der Benachrichtigungsvorlage identisch mit dem einer Standardvorlage ist, erzeugt eine benutzerdefinierte Senderadresse eine benutzerdefinierte Vorlage für eine bestimmte Benachrichtigung.

Minimieren der Anzahl der Abonnements.

Zur verbesserten Leistung eines Benachrichtigungsservice 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 Nachrichtenvorlagen entspricht, kann das System die Verteilung nicht effizient zusammenfassen und muss separate Hinweisnachrichten 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 Benutzerdokumentation zu IBM SPSS Deployment Manager. 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 Nachrichtenverarbeitung und Verteilungszeit zu minimieren.

Planen von Aktiviäten zur Abonnementverwaltung.

Zur verbesserten Leistung beim Ereignisabgleich führt der Benachrichtigungsservice von IBM SPSS Collaboration and Deployment Services eine Reihe von internen Caches. Diese Caches werden ungültig (gelöscht), wenn der Client Änderungen am Ereignistyprepository oder am Abonnementrepository 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 Benachrichtigungsservice liegt. Das Ausführen der Abonnementverwaltung bei geringer Verarbeitungslast ist im Allgemeinen akzeptabel, kann aber zu kurzzeitigen Leistungsabfällen führen.

Fehlersuche im Benachrichtigungsservice

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

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

Andere Anwendungsserver können Browserschnittstellen oder einige andere Bearbeitungmöglichkeiten für die Protokollierungskonfiguration der eingesetzten Komponenten zur Verfügung stellen. Um die SMTP-Protokollierung zu aktivieren, stellen Sie die Konfigurationsoption *SMPT - Debugmodus einschalten* in IBM SPSS 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 richtige Einstellungen und die E-Mail-Adresse des Standardabsenders bei der Installation des Repositorys angegeben wurden, ist in der Regel keine zusätzliche E-Mail-Konfiguration erforderlich, damit Benachrichtigungen von IBM SPSS Collaboration and Deployment Services erfolgreich zugestellt werden. Wenn bei der Installation ein Fehler unterlaufen ist, kann dieser durch Ändern der Konfigurationsoptionen für Benachrichtigungen korrigiert werden. Weitere Informationen finden Sie im Thema „Benachrichtigung” auf Seite 45.

Der Administrator für IBM SPSS Collaboration and Deployment Services wird ebenfalls über die fehlgeschlagene Zustellung von Benachrichtigungen oder Abonnements mit einer systemgenerierten Nachricht 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 Hinweisnachrichten aufgrund der Einrichtung des Unternehmensnetzes 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. Fehlgeschlagene Zustellungen von Benachrichtigungen und Abonnements werden in Repository-Auditing-Ansichten protokolliert. Weitere Informationen finden Sie in Kapitel 15, „Auditing des Repositorys”, auf Seite 89.

- Um die Ursache der fehlgeschlagenen Benachrichtigung zu bestimmen, sollten Sie den Debugging-Modus aktivieren. Weitere Informationen finden Sie im Thema „Fehlersuche im Benachrichtigungsservice" auf Seite 84.
- **nslookup**-Abfragen können verwendet werden, um die Konfiguration Ihres SMTP-Servers zu prüfen.
- Eine Überprüfung der SMTP-Header der Hinweisnachrichten kann nützliche Informationen zur Nachrichtenweiterleitung des SMTP-Servers liefern.

Kapitel 14. JMS-Konfiguration für Prozessmanagement

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

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 Grenzwerte für gemeinsamen Zugriff

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 und JBoss beschrieben. Detailliertere Informationen finden Sie in der Dokumentation zum Anwendungsserver.

WebSphere

1. Wählen Sie in WebSphere Integrated Solutions Console folgende Optionen aus:

   Resources > **JMS** > **Activation Specifications**
2. Öffnen Sie **`CaDSProcessEventActivationSpec`** und erhöhen Sie den Wert von `Maximum concurrent MDB invocations per endpoint`.
3. Starten Sie den Server erneut.

JBoss

1. Erhöhen Sie den Wert des Elements **`MaximumSize`** in `<JBoss-Serververzeichnis>/conf/standardjboss.xml`.

   Im folgenden Beispiel wird der Wert von **`MaximumSize`** auf 150 gesetzt (der Standardwert ist 15).

```
<invoker-proxy-binding>
      <name>message-driven-bean</name>
      <invoker-mbean>default</invoker-mbean>
      <proxy-factory>org.jboss.ejb.plugins.jms.JMSContainerInvoker</proxy-factory>
      <proxy-factory-config>
        <JMSProviderAdapterJNDI>DefaultJMSProvider</JMSProviderAdapterJNDI>
        <ServerSessionPoolFactoryJNDI>StdJMSPool</ServerSessionPoolFactoryJNDI>
        <CreateJBossMQDestination>true</CreateJBossMQDestination>
        <!-- WARN: Don't set this to zero until a bug in the pooled executor is fixed -->
        <MinimumSize>1</MinimumSize>
        <MaximumSize>150</MaximumSize>
        <KeepAliveMillis>30000</KeepAliveMillis>
        <MaxMessages>1</MaxMessages>
        <MDBConfig>
```

```
        <ReconnectIntervalSec>10</ReconnectIntervalSec>
        <DLQConfig>
          <DestinationQueue>queue/DLQ</DestinationQueue>
          <MaxTimesRedelivered>200</MaxTimesRedelivered>
          <TimeToLive>0</TimeToLive>
        </DLQConfig>
      </MDBConfig>
    </proxy-factory-config>
  </invoker-proxy-binding>
```

2. Starten Sie den Server erneut. Die Änderung wirkt sich auf alle bereitgestellten nachrichtengesteuerten Beans aus.

Beispiel für nachrichtenbasierte Verarbeitung

Die nachrichtenbasierte 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-Datenstrom aktualisiert wird.

Dieses Verfahren beinhaltet die folgenden Schritte:

1. Erstellen Sie über IBM SPSS Deployment Manager eine JMS-Nachrichtendomäne.
2. Richten Sie mithilfe der Nachrichtendomäne einen nachrichtenbasierten Zeitplan für den Job ein. Beachten Sie, dass die Nachrichtenauswahl die Ressourcen-ID des IBM SPSS Modeler-Datenstroms wie im folgenden Beispiel angeben muss:

   ```
   ResourceID=<Ressourcen-ID>
   ```

   Die Repository-Ressourcen-ID des IBM SPSS Modeler-Datenstroms befindet sich in den Objekteigenschaften.
3. Richten Sie auf Basis des von Ihnen definierten JMS-Abonnenten eine Benachrichtigung für den IBM SPSS Modeler-Datenstrom ein.
4. Um den nachrichtenbasierten Zeitplan zu testen, muss der Datenstrom in IBM SPSS Modeler geöffnet, geändert und im Repository gespeichert werden. Wenn alles korrekt eingestellt wurde, wird der Zeitplan den Job auslösen.

Kapitel 15. Auditing des Repositorys

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 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.

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

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.

Datenbankauditfunktionen

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 Datenbankclientanwendung.

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 zu Repository-Objekten abrufen lässt, z. B. Dateien, Jobs, Datenströme 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: Auditabfragen können für Ereignistabellen von IBM SPSS Collaboration and Deployment Services sowie für vordefinierte Ansichten ausgeführt werden. Da sich die Tabellenstruktur jedoch in späteren

Systemversionen ändern kann, empfiehlt es sich aus Kompatibilitätsgründen beim Schreiben von Auditabfragen Ansichten anstelle von Tabellen zu verwenden.

Auditereignisse

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

Jobausführungsereignisse

- 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 Auditereignistabellen (SPSSAUDIT_EVENTS) und Ereignisparametertabellen (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 Eins-zu-viele-Beziehung).

Auditereignistabelle (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 - Benutzerauthentifizierungsereignis
- security/componentLRU - Benutzer- und Gruppen-Setup-Ereignis
- prms/prms - Jobplanungsereignis
- notification/notification - Benachrichtigungs- oder Abonnementereignis
- userpref/auditComponent - Ereignis für Änderung von Benutzervorgaben
- 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, die/der erstellt wurde
- repository/audit_update_object - Datei oder Ordner, die/der aktualisiert wurde (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 für 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 - Vorhandene 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 - Kennwortänderung
- security/locLRUAdd - Gruppe hinzugefügt
- security/locLRUUpdate - Gruppe umbenannt
- security/locLRUUpdate - Benutzer zu Gruppe hinzugefügt/aus Gruppe gelöscht
- security/locLRUDelete - Gruppe gelöscht

Locus-Codes für Jobausführungsereignisse

- prms/audit_job_submit - Job übergeben
- prms/audit_job_start - Job gestartet

- prms/audit_job_step_start - Jobschritt gestartet
- 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 Hinweisnachricht (zugestellt, nicht zugestellt oder teilweise zugestellt)
- notification/audit_subscription - Änderungsereignis für Benachrichtigungs- oder Abonnementeinstellungen (Abonnement erstellt, aktualisiert oder gelöscht)

Locus-Codes für Benutzervorgabeereignisse
- userpref/auditLSet - Benutzervorgabewert festgelegt
- userpref/auditLDelete - Benutzervorgabewert 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. Eine Zeichenfolge, die zusätzliche komponentendefinierte Informationen zu dem Ereignis liefert, z. B. eine alte Beschriftung bei einer Beschriftungsänderung, 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.

Auditereignisparametertabelle (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 Datenbankclientanwendung, um zusätzliche Informationen zu den Eigenschaften von Ereignistabellen zu beziehen, z. B. Spaltendatentypen und "Nullability".

Auditansichten

Die folgenden Auditansichten werden bei der Installation des Repositorys standardmäßig in der Datenbank erstellt. Nutzen Sie Tools der Datenbankclientanwendung, 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 Auditansichten verwendet werden. Die Unterstützungsansichten sind nicht für Berichterstellungen vorgesehen.

Audit (SPSSPLAT_V_AUDIT)

Die Auditansicht enthält Auditing-Informationen aus der Ansicht "Dateiversion". Diese Ansicht enthält eine Zeile für jeden Auditparameter für jedes Auditereignis.

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

AUDITTIMESTAMP. Die Auditzeitmarke (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 Principalbenutzer des Objekts, für das Auditing durchgeführt wird.

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

AUDITDETAILS. Eine Zeichenfolge, die zusätzliche komponentendefinierte Informationen zu dem Ereignis liefert, z. B. eine alte Beschriftung bei einer Beschriftungsänderung, 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 zur Datei- oder Jobversionsmarkierung 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" (Eins-zu-viele-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-Datenströme, 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. Die Versionsmarkierung der Dateiversion.

VERSIONLABEL. Die Versionsbeschriftung 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-Erfolgreich
- 2-In Warteschlange
- 3-In Verarbeitung
- 4-Beendet
- 5-Weiterleiten
- 6-Fehler
- 7-Fehler weitergeben
- 8-Mit Abbruchsanforderung
- 9-Abgebrochen
- 10-Abbruch anstehend
- 11-Weitergabe 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 Zeichenfolgewert, 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 zu Jobschritten 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-Datenstrom, eine IBM SPSS Statistics- oder SAS-Syntaxdatei usw.

REFERENCEDFILELABEL. Die Beschriftung 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 die Jobbeschriftung 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. Beschriftung des Jobs, der beim Auslösen des Zeitplans ausgeführt werden soll.

SCHEDULELASTUPDATE. Die Zeitmarke für das Datum, an dem dieser Zeitplan zuletzt geändert wurde.

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

Datenstromattributwert (SPSSPLAT_V_STREAMATTRVALUE)

Die Ansicht "Datenstromattributwert" präsentiert die Attributinformationen zu den Knoten in einem IBM SPSS Modeler-Datenstrom. Diese Ansicht enthält eine Zeile für jeden zulässigen Wert eines jeden Attributs in jedem Datenstrom.

ATTRIBUTEID. Die eindeutige ID des Attributs.

ATTRIBUTENAME. Der Name des Attributs.

NODEID. Fremdschlüssel zum Knoten in der Ansicht "Datenstromknoten".

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.

Datenstromknoten (SPSSPLAT_V_STREAMNODE)

Die Ansicht "Datenstromknoten" präsentiert die Informationen für die Knoten in IBM SPSS Modeler-Datenströmen. Diese Ansicht enthält eine Zeile für jeden Knoten in jeder Version jedes Datenstroms.

NODEID. Die eindeutige ID des Knotens im Datenstrom.

STREAMID. Fremdschlüssel zum Datenstrom (FILEID) in der Ansicht "Dateiversion", die diesen Knoten enthält.

STREAMVERSION. Fremdschlüssel zur Datenstromversion in der Ansicht "Dateiversion", die diesen Knoten enthält.

NODENAME. Der Name des Knotens im Datenstrom.

NODETYPE. Der Typ des Knotens im Datenstrom.

NODELABEL. Die Beschriftung des Knotens im Datenstrom.

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.

Anmerkung: In diesem Release werden die Spalten ioDSN und ioDATABASETABLE in der Ansicht SPSSPLAT_V_STREAMNODE nicht verwendet. Diese Spalten enthalten 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

Protokollierungstabelle für Anforderungen

Standardmäßig werden die Scoring-Serviceanforderungsdaten in der Tabelle SPSSSCORE_LOG gespeichert. Jede Zeile in der Tabelle entspricht einer Anforderung des Scoring-Service.

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. Weitere Informationen finden Sie im Thema „XML-Schema" auf Seite 101. 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, sodass 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 Repositorys 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 Datenbankclientanwendung, 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 der Lastausgleichsfunktion für den Cluster oder des 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 in der browserbasierten Instanz von IBM SPSS Deployment Manager so eingestellt wird, dass es den Hostnamen nicht nachschlägt.

PRINCIPAL. 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 die Zeitmarke 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-Datenstrom für das Scoring konfiguriert wurde, ist das die Repository-ID des Datenstroms.

MODEL_VERSION_MARKER. Die ID 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_INPUT steht für einen einzelnen Eingabewert.

SERIAL. Die eindeutige ID der Scoring-Anforderungszeile.

INPUT_TABLE. Der Tabellenname.

INPUT_NAME. Der Name eines Eingabefelds.

INPUT_VALUE. Eingabewert.

INPUT_TYPE. Der Eingabedatentyp. Die folgenden Datentypen sind zulässig:

- date
- daytime
- decimal
- double
- float
- integer

- long
- string
- timestamp

Kontextdaten der Scoring-Anforderung (SPSSSCORE_V_LOG_CONTEXT_INPUT)

Diese Ansicht enthält Informationen zu den Daten, die an den Scoring-Service übergeben wurden. 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. Eingabewert.

Eingabe für die Scoring-Anforderung (SPSSSCORE_V_LOG_REQUEST_INPUT)

Diese Ansicht enthält die Informationen zu den Daten, die als Eingabe für die Anforderung des Scoring-Service verwendet werden.

SERIAL. Die eindeutige ID der Scoring-Anforderungszeile.

RI_TABLE. Der Name der in der Anforderung verwendeten Tabelle.

RI_ROW. Die Zeilennummer der Anforderungsdatenzeile beginnend mit der Zahl 1.

RI_NAME. Der Name eines Eingabefelds, der dem Namen der Spalte in der Anforderung entspricht.

RI_VALUE. Eingabewert.

Eigenschaften der Scoring-Anforderung (SPSSSCORE_V_LOG_REQUEST_PROP)

Diese Ansicht enthält die Informationen zu den Eigenschaften, die einer Eingabetabelle zugeordnet sind.

SERIAL. Die eindeutige ID der Scoring-Anforderungszeile.

RI_TABLE. Der Name der in der Anforderung verwendeten Tabelle.

RI_PROP_NAME. Der Name der Eigenschaft.

RI_PROP_VALUE. Der Wert der Eigenschaft.

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. Ausgabewert.

Metriken für die Scoring-Anforderung (SPSSSCORE_V_LOG_METRIC)

Die Ansicht SPSSSCORE_V_LOG_METRIC wird verwendet, um die Ausgabemetriken 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 Metrikfelds.

METRIC_VALUE. Metrikwert.

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.

PROPERTY_NAME. Der Name einer Eigenschaft.

PROPERTY_VALUE. Eigenschaftswert.

XML-Schema

Das folgende XML-Schema wird in der Datenbank registriert und für die Spalte `INFO` der Tabelle `SPSSSCORE_LOG` verwendet. Dieses Schema ist für MS SQL Server und Oracle erforderlich. Unter Db2 ist es nicht erforderlich.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
    attributeFormDefault="unqualified"
    elementFormDefault="qualified"
    targetNamespace="http://xml.spss.com/scoring/logging"
    version="2.0"
    jaxb:version="2.0"
    xmlns:jaxb="http://java.sun.com/xml/ns/jaxb"
    xmlns:spss_ss_logging="http://xml.spss.com/scoring/logging"
    xmlns:xs="http://www.w3.org/2001/XMLSchema">

    <!-- ************************************************************** -->
    <!-- SIMPLE TYPES                                                   -->
    <!-- ************************************************************** -->
    <xs:simpleType name="pevDataType">
        <xs:annotation>
            <xs:documentation>The type of this column. This maps to the same types defined by
              the DD EventServer. We will map these types to the SQL types using the same
              mapping that the DD Event Server uses.</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="boolean"/>
            <!--    <xs:enumeration value="character"></xs:enumeration> not needed, as string
                    should be sufficient for mapping to SQL -->
            <xs:enumeration value="date"/>
            <xs:enumeration value="daytime"/>
            <xs:enumeration value="decimal"/>
            <xs:enumeration value="double"/>
            <xs:enumeration value="float"/>
            <xs:enumeration value="integer"/>
            <xs:enumeration value="long"/>
            <xs:enumeration value="string"/>
            <xs:enumeration value="timestamp"/>
```

```
    </xs:restriction>
</xs:simpleType>

<xs:attributeGroup name="nillableValueAttributeGroup">
    <xs:attribute name="value" type="xs:string" use="optional">
        <xs:annotation>
            <xs:documentation>A value, in string representation.  If this attribute is not
            specified, the value is considered to be null.  The text representation of the
            numeric types is obvious, but several types are not.  The format of the
            non-numeric types must be as follows: boolean='true'(case insensitive) or '1'
            or 'false'(case insensitive) or '0', date='yyyy-MM-dd', daytime='HH:mm:ss', and
            timestamp='yyyy-MM-ddTHH:mm:ss'.</xs:documentation>
        </xs:annotation>
    </xs:attribute>
</xs:attributeGroup>

<!-- ************************************************************** -->
<!-- COMPLEX TYPES                                                  -->
<!-- ************************************************************** -->
<xs:complexType name="modelInputValue">
    <xs:annotation>
        <xs:documentation>This element is optionally returned as part of the scoreResult
        element.  If the configuration is programmed to return the model input fields
        (see spss_ss:modelInputMetadataField), then this element contains the value that
        was used to produce the score.  The value might be null.</xs:documentation>
    </xs:annotation>
    <xs:attribute name="name" type="xs:string" use="required">
        <xs:annotation>
            <xs:documentation>The name of the input item.</xs:documentation>
        </xs:annotation>
    </xs:attribute>
    <xs:attribute name="type" type="spss_ss_logging:pevDataType" use="required">
        <xs:annotation>
            <xs:documentation>The data type of the input item.</xs:documentation>
        </xs:annotation>
    </xs:attribute>
    <xs:attributeGroup ref="spss_ss_logging:nillableValueAttributeGroup"/>
</xs:complexType>

<xs:complexType name="inputTable">
    <xs:annotation>
        <xs:documentation>One table of input values, may contain zero or more
        rows.</xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="columns" type="spss_ss_logging:inputColumn" minOccurs="1"
        maxOccurs="unbounded">
            <xs:annotation>
                <xs:documentation>An ordered list of column names</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="rowValues" type="spss_ss_logging:rowValues" minOccurs="0"
        maxOccurs="unbounded">
            <xs:annotation>
                <xs:documentation>A row of values, value order must match defined column
                order.</xs:documentation>
            </xs:annotation>
        </xs:element>
    </xs:sequence>
    <xs:attribute name="sourceTable" type="xs:string" use="required">
        <xs:annotation>
            <xs:documentation>This attribute holds the name of the source table as defined
            in the model.</xs:documentation>
        </xs:annotation>
    </xs:attribute>
</xs:complexType>

<xs:complexType name="inputColumn">
    <xs:annotation>
        <xs:documentation>Describes a column in the designated input table.  If the
        configuration is programmed to return the model input fields (see
        spss_ss:modelInputMetadataField), then this element contains the value that
        was used to produce the score.  The value might be null.</xs:documentation>
    </xs:annotation>
    <xs:attribute name="name" type="xs:string" use="required">
        <xs:annotation>
            <xs:documentation>The name of the input item.</xs:documentation>
        </xs:annotation>
    </xs:attribute>
    <xs:attribute name="type" type="spss_ss_logging:pevDataType" use="required">
        <xs:annotation>
            <xs:documentation>The data type of the input item.</xs:documentation>
        </xs:annotation>
    </xs:attribute>
```

```
</xs:complexType>

<xs:complexType name="inputTableWithProperties" >
    <xs:annotation>
        <xs:documentation>Input tables can have loggable properties</xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="spss_ss_logging:inputTable">
            <xs:sequence>
                <xs:element name="RequestInputProperties"
                type="spss_ss_logging:requestInputProperties" minOccurs="0" maxOccurs="1">
                    <xs:annotation>
                        <xs:documentation>Properties that are associated with an input
                        table</xs:documentation>
                    </xs:annotation>
                </xs:element>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>

<xs:complexType name="requestInputProperties">
    <xs:annotation>
        <xs:documentation>Properties that are associated with an input table</xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="property" type="spss_ss_logging:nameValueType" minOccurs="1"
        maxOccurs="unbounded">
            <xs:annotation>
                <xs:documentation>Properties that are associated with an input
                table</xs:documentation>
            </xs:annotation>
        </xs:element>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="columnNames">
    <xs:annotation>
        <xs:documentation/>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="rowValues">
    <xs:annotation>
        <xs:documentation>One row of values, note that a value may be nill.</xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="value" type="spss_ss_logging:nillableValue" minOccurs="1"
        maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="output">
    <xs:sequence>
        <xs:element name="columnNames" type="spss_ss_logging:columnNames">
            <xs:annotation>
                <xs:documentation>An ordered list of column names</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="rowValues" type="spss_ss_logging:rowValues" minOccurs="1"
        maxOccurs="unbounded">
            <xs:annotation>
                <xs:documentation>A row of score data, following the order in the
                columnNames element</xs:documentation>
            </xs:annotation>
        </xs:element>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="nameValueType">
    <xs:annotation>
        <xs:documentation>A name value pair.</xs:documentation>
    </xs:annotation>
    <xs:attribute name="name" type="xs:string" use="required"/>
    <xs:attribute name="value" type="xs:string" use="required"/>
</xs:complexType>

<xs:complexType name="context">
    <xs:annotation>
        <xs:documentation>This element contains all the context data inputs to the score
        request.</xs:documentation>
```

```
    </xs:annotation>
    <xs:sequence>
        <xs:element name="columnNames" type="spss_ss_logging:columnNames">
            <xs:annotation>
                <xs:documentation>An ordered list of column names</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="rowValues" type="spss_ss_logging:rowValues" minOccurs="1"
        maxOccurs="unbounded">
            <xs:annotation>
                <xs:documentation>A row of context data, following the order in the
                columnNames element</xs:documentation>
            </xs:annotation>
        </xs:element>
    </xs:sequence>
    <xs:attribute name="table" type="xs:string" use="required">
        <xs:annotation>
            <xs:documentation>This attribute describes which context table the input data
            belongs to.</xs:documentation>
        </xs:annotation>
    </xs:attribute>
</xs:complexType>

<xs:complexType name="nillableValue">
    <xs:annotation>
        <xs:documentation>Nillable elements and simpleTypes are not well supported by most
        of the popular frameworks, especially Castor.  Instead of a nillable string element,
        use an optional string attribute to represent null values.</xs:documentation>
    </xs:annotation>
    <xs:attributeGroup ref="spss_ss_logging:nillableValueAttributeGroup"/>
</xs:complexType>

<!-- ================================================================ -->
<!-- ELEMENTS                                                         -->
<!-- ================================================================ -->
<xs:element name="Info">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="Output" type="spss_ss_logging:output" minOccurs="0" maxOccurs="1">
                <xs:annotation>
                    <xs:documentation>PA has the ability to generate multiple outputs
                    (multiple offers).  There will be one OutputRow for each output
                    (for each offer). </xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="ContextInput" type="spss_ss_logging:context" minOccurs="0"
            maxOccurs="unbounded">
                <xs:annotation>
                    <xs:documentation>Context data that is fed into the data engine
                    and not necessarily into the model.  </xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="RequestInputs" type="spss_ss_logging:inputTableWithProperties"
            minOccurs="0" maxOccurs="unbounded">
                <xs:annotation>
                    <xs:documentation>Zero to N score request input tables. The data
                    contained in each table represents the inputs provided with the score
                    request.</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="Metric" type="spss_ss_logging:nameValueType" minOccurs="0"
            maxOccurs="unbounded">
                <xs:annotation>
                    <xs:documentation>A metric which is defined by either the HSS engine
                    or the provider.
                    Value is a double represented as a string to account for the
                    correct precision and scale.
                    An example might be the time to produce the output.</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="Property" type="spss_ss_logging:nameValueType" minOccurs="0"
            maxOccurs="unbounded">
                <xs:annotation>
                    <xs:documentation>A property value.  The name is the name of the
                    property.</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="ModelObjectId" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="ModelVersionMarker" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="ConfigurationName" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="ModelInputTable" type="xs:string" minOccurs="0" maxOccurs="1">
                <xs:annotation>
                    <xs:documentation>THIS ELEMENT IS NOW DEPRECATED.</xs:documentation>
                </xs:annotation>
```

```
            </xs:element>
          </xs:sequence>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

Beispiele für Auditabfragen

Nachfolgend erhalten Sie Beispiele für SQL-Abfragen in Auditansichten. Beachten Sie, dass bestimmte SQL-Funktionen für Microsoft SQL Server 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'
```

Kapitel 16. nativestore-Schema - Referenz

Das Schema *nativestore.xsd* definiert die Struktur einer XML-Datei, die Benutzer und Gruppen enthält, die in IBM SPSS Collaboration and Deployment Services 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 xmlns="spssnative">
  <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)

Stammelement für den Import von lokalen Benutzern und ihren Gruppen in IBM SPSS Collaboration and Deployment Services.

Untergeordnete Elemente

user, obsolete

user (Element)

Benutzer wird hinzugefügt oder aktualisiert.

Übergeordnetes Element

nativestore

Untergeordnete Elemente

group, role

Attribute

Tabelle 19. Attribute für das Element "user".

Name	Typ	Verwendung	Standard	Beschreibung
`userID`	string	erforderlich	*kein Standardwert*	Benutzer-ID, die für die Anmeldung beim System verwendet wird.

Tabelle 19. Attribute für das Element "user" (Forts.).

Name	Typ	Verwendung	Standard	Beschreibung
password	string	optional	*kein Standardwert*	Für gewöhnlich ein unverschlüsseltes Kennwort. Wenn das Attribut encrypted auf "true" gesetzt ist, wird dieses Kennwort verschlüsselt. Für gewöhnlich ist es nicht möglich, beim Import ein verschlüsseltes Kennwort zu verwenden. Kennwörter werden beim Export vom Server verschlüsselt, dies wird in den IBM SPSS Collaboration and Deployment Services-Benutzerschnittstellen jedoch *nicht* dargestellt.
encrypted	boolean	optional	false	Zeigt an, ob das Kennwort Standardtext oder verschlüsselt ist. Verschlüsselte Kennwörter werden aus dem Native Store exportiert (dies ist eine Einwegverschlüsselung, die eine Wiederherstellung eines Benutzerkennworts unmöglich macht). Beim Import aus einem anderen System müssen Kennwörter in Standardtext gehalten sein; das Attribut encrypted wird für gewöhnlich weggelassen.

Beispiel-XML

```
<?xml version="1.0" encoding="UTF-8"?>
<nativestore xmlns="spssnative">
  <user userID="sbennett" password="sb9482" encrypted="false">
    <group>sales</group>
  </user>
</nativestore>
```

group (Element)

Gruppen, die mit dem Benutzer verknüpft sind. Falls eine Gruppe nicht vorhanden ist, wird sie automatisch erstellt.

Typ: Zeichenfolge

Übergeordnetes Element

user

Beispiel-XML

```
<?xml version="1.0" encoding="UTF-8"?>
<nativestore xmlns="spssnative">
  <user userID="sbennett" password="sb9482" encrypted="false">
    <group>sales</group>
  </user>
</nativestore>
```

role (Element)

Rolle, die mit dem Benutzer verknüpft ist. Falls eine Rolle nicht vorhanden ist, wird sie *nicht* automatisch hinzugefügt.

Typ: Zeichenfolge

Übergeordnetes Element

user

obsolete (Element)

Gruppen oder Benutzer, die entfernt werden sollen. Beachten Sie, dass sie im Ersetzungsmodus geladen werden können, der automatisch alle Gruppen und nicht administrativen Benutzer entfernt. In diesem Modus hat dieses Element keine Wirkung.

Übergeordnetes Element

nativestore

Untergeordnete Elemente

user, group

Beispiel-XML

```
<?xml version="1.0" encoding="UTF-8"?>
<nativestore xmlns="spssnative">
  <obsolete>
    <user>mmonroe</user>
    <user>bgmurphy</user>
    <group>jones project</group>
  </obsolete>
</nativestore>
```

user (Element)

Die Benutzer-ID, die entfernt werden soll. Benutzer mit Administratorberechtigungen können nicht entfernt werden.

Typ: Zeichenfolge

Übergeordnetes Element

obsolete

Beispiel-XML

```
<?xml version="1.0" encoding="UTF-8"?>
<nativestore xmlns="spssnative">
  <obsolete>
    <user>mmonroe</user>
  </obsolete>
</nativestore>
```

group (Element)

Gruppenname, der entfernt werden soll.

Typ: Zeichenfolge

Übergeordnetes Element

obsolete

Beispiel-XML

```
<?xml version="1.0" encoding="UTF-8"?>
<nativestore xmlns="spssnative">
  <obsolete>
    <group>jones project</group>
  </obsolete>
</nativestore>
```

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. IBM stellt dieses Material möglicherweise auch in anderen Sprachen zur Verfügung. Für den Zugriff auf das Material in einer anderen Sprache kann eine Kopie des Produkts oder der Produktversion in der jeweiligen Sprache erforderlich sein.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Die angeführten Leistungsdaten und Kundenbeispiele dienen nur zur Illustration. Die tatsächlichen Ergebnisse beim Leistungsverhalten sind abhängig von der jeweiligen Konfiguration und den Betriebsbedingungen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis) und ohne jegliche Gewährleistung zur Verfügung gestellt. IBM übernimmt keine Haftung für Schäden, die durch die Verwendung der Beispielprogramme entstehen.

Hinweise zur Datenschutzrichtlinie

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Dieses Softwareangebot verwendet keine Cookies oder andere Technologien zur Erfassung personenbezogener Daten.

Wenn es die für dieses Softwareangebot bereitgestellten Konfigurationen Ihnen als Kunde ermöglichen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in der "IBM Online-Datenschutzerklärung, Schwerpunkte" unter http://www.ibm.com/privacy, in der "IBM Online-Datenschutzerklärung" unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und in "IBM Software Products and Software-as-a-Service Privacy Statement" unter http://www.ibm.com/software/info/product-privacy.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corp in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

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

Intel, das Intel-Logo, Intel Inside, das Intel Inside-Logo, Intel Centrino, das Intel Centrino-Logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium und Pentium sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA oder 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 der 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 auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

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

Index

F

G

H

I

J

K

L

M

W

X

Z

Gedruckt in Deutschland