IBM SPSS Collaboration and Deployment Services Repository
Version 8 Release 2

Installations- und Konfigurationshandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 73 gelesen werden.

Produktinformation

Diese Ausgabe bezieht sich auf Version 8, Release 2, Modifikation 0 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

Der Begriff *Zusammenarbeit* (Collaboration) bezeichnet die Möglichkeit, analytische Informationen effizient gemeinsam zu verwenden und wiederzuverwenden. Außerdem ist die Zusammenarbeit der Schlüssel zum Erstellen und Implementieren von Analysen in Unternehmen.

Analysten benötigen einen Ort, an dem sie Dateien ablegen können, die anderen Analysten oder Fachanwendern zur Verfügung gestellt werden sollen. Sicherheit ist erforderlich, um den Zugriff auf die Dateien und das Ändern der Dateien zu steuern. 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. Analysten können eine Version einer Datei im Entwicklungsstadium speichern, diese Version zu einem späteren Zeitpunkt abrufen und mit deren Bearbeitung fortfahren, bis diese fertiggestellt ist und in der Produktion verwendet werden kann. Zu diesen Dateien können benutzerdefinierte Schnittstellen gehören, die Analyseprozesse ausführen, sodass Fachanwender von der Arbeit eines Analysten profitieren können.

Der Einsatz des Repositorys schützt das Unternehmen, indem es einen zentralen Speicherort für Analyseassets bietet, der sich bequem sichern und wiederherstellen lässt. Des Weiteren steuern Berechtigungen auf Benutzer-, Datei- und Versionsbeschriftungsebene den Zugriff auf einzelne Informationen. Versions-

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

Bereitstellung

Damit die Vorteile der Vorhersageanalyse voll ausgeschöpft werden können, müssen die analytischen Informationen bei Geschäftsentscheidungen verfügbar sein. 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 das Scoring konfiguriertes Analysemodell kann Daten aus einem aktuellen Kundenkontakt mit historischen Daten kombinieren, um einen Score zu bilden, der den Verlauf des Kontakts bestimmt. Der Service selbst kann von jeder Clientanwendung verwendet werden, sodass die Erstellung benutzerdefinierter Schnittstellen zum Definieren des Prozesses möglich wird.

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 müssen Berechtigungsnachweise in verschiedenen Phasen des Prozesses nicht manuell bereitgestellt werden. Darüber hinaus kann das System so konfiguriert werden, dass es mit dem Federal Information Processing Standard Publication 140-2 konform ist.

Systemarchitektur

Im Allgemeinen besteht IBM SPSS Collaboration and Deployment Services aus einer einzigen, zentralen Instanz von IBM SPSS Collaboration and Deployment Services Repository, die über Ausführungsserver zum Verarbeiten von analytischen Informationen eine ganze Reihe von Clients bedient.

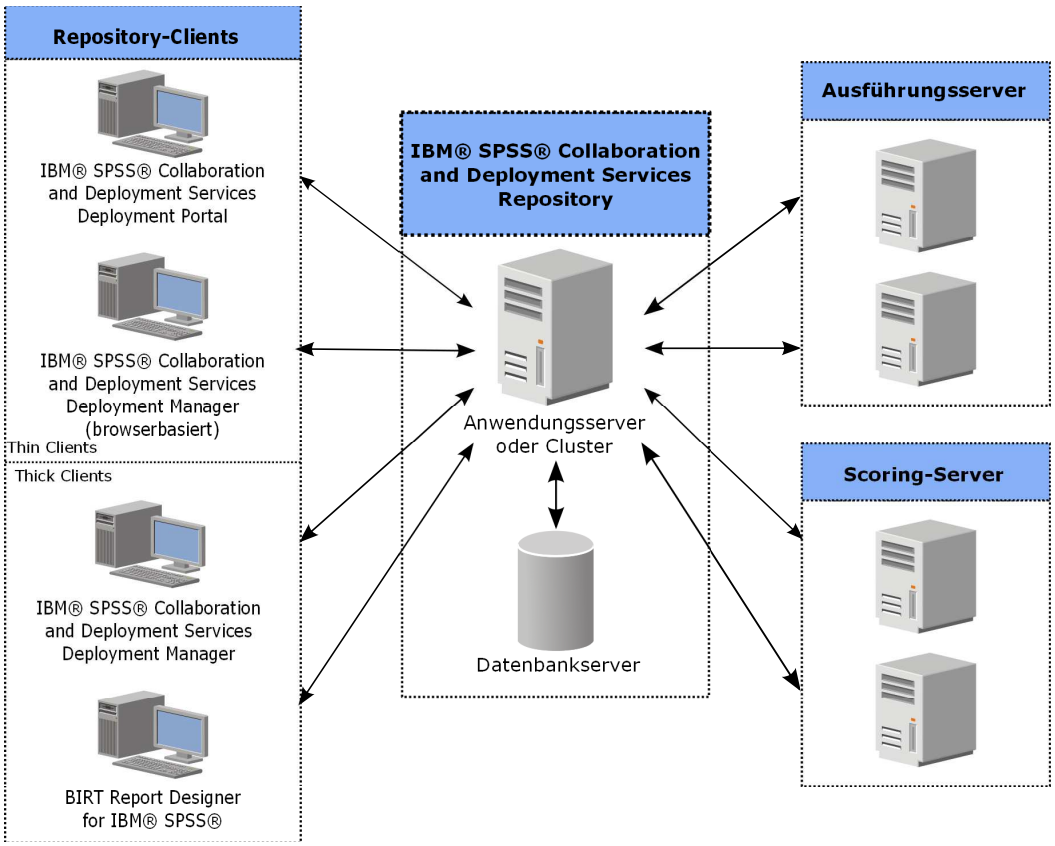

Abbildung 1. Architektur von IBM SPSS Collaboration and Deployment Services

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.

IBM SPSS Collaboration and Deployment Services unterstützt folgende Ausführungsserver:

- **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 sind 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, Masterdaten-Management und Funktionen zur Prozessautomatisierung von IBM SPSS Collaboration and Deployment Services zur Optimierung und Automatisierung von Entscheidungen mit hohem Volumen sowie zum Erstellen verbesserter Ergebnisse in bestimmten Geschäftssituationen.

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 für Installationsverantwortliche

IBM SPSS Collaboration and Deployment Services Repository 8.2 stellt neue Funktionen bereit, die die Bereitstellung von Vorhersageanalysen erleichtern und Ihnen helfen, die Kosten besser in den Griff zu bekommen.

Unterstützung für weitere Plattformen

IBM SPSS Collaboration and Deployment Services Repository 8.2 beinhaltet Unterstützung für neue Versionen von Betriebssystemen (einschließlich AIX 7.1 und Ubuntu 16.04 LTS s390x), Anwendungsservern, Datenbanken, Virtualisierungsumgebungen und Web-Browsern.

IBM WebSphere Application Server Liberty Profile für IBM SPSS Collaboration and Deployment Services Repository

IBM SPSS Collaboration and Deployment Services Repository enthält WebSphere Application Server Liberty Profile, um die Installation und die Bereitstellung zu vereinfachen. Sie können entweder diesen Anwendungsserver für eine Standalone- oder Clusterinstallation verwenden oder eine eigene Anwendungsserverinstanz bereitstellen.

Vereinfachter und automatisierter Installations- und Konfigurationsprozess für IBM SPSS Collaboration and Deployment Services Repository

Ein neues Installationsprogramm bietet einen vereinfachten Installations- und Konfigurationsprozess durch Nutzung der vollständige Funktionalität von IBM Installation Manager an.

Änderungen in diesem Release

Oracle WebLogic Server wird nicht mehr unterstützt.

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 dieses Featuremöglicherweise 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

Tabelle 1. Veraltete Features aus Vorgängerversionen (Forts.)

Einstellung der Unterstützung	**Empfohlene Migrationsaktion**
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
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. Installation

Dieses Kapitel enthält die Informationen zur Installation von IBM SPSS Collaboration and Deployment Services Repository. Der Vorgang umfasst mehrere Schritte vor der Installation, während der Installation und Konfiguration sowie nach der Installation.

- Die **Schritte vor der Installation** zum Einrichten der Anwendungsumgebung umfassen das Bestimmen der Systemanforderungen basierend auf dem Installationstyp und der geplanten Systemverwendung, das Bereitstellen der Computer zum Ausführen des Anwendungsservers oder des Server-Clusters, das Sicherstellen der Einhaltung aller Hardware- und Softwareanforderungen durch die Server, das Konfigurieren des Anwendungsservers oder Clusters und das Konfigurieren der Datenbank. Ferner kann auch das Migrieren des Inhalts aus der vorherigen Installation mithilfe der Datenbankkopiertools in die neue Datenbank erforderlich sein.
- Die **Installations- und Konfigurationsschritte** umfassen das Installieren der Anwendungsdateien auf dem Hostsystem mit IBM Installation Manager und die anschließende Konfiguration von IBM SPSS Collaboration and Deployment Services Repository zur Ausführung mit dem vorgesehenen Anwendungsserver oder Server-Cluster und der Repository-Datenbank.
- Die **Schritte nach der Installation** umfassen das Starten von IBM SPSS Collaboration and Deployment Services Repository, das Prüfen der Konnektivität, das Konfigurieren des automatischen Startens und das Installieren von zusätzlichen Datenbanktreibern, optionalen Komponenten und Content-Adaptern für andere IBM SPSS-Produkte.

Beachten Sie, dass für die Bereitstellung von IBM SPSS Collaboration and Deployment Services Repository in manchen Umgebungen auch einige optionale Unternehmenskonfigurationsschritte für die Anwendungssicherheit, die Zugriffssteuerung und die Benachrichtigungsfunktionen erforderlich sein können.

- E-Mail und RSS-Benachrichtigungen. Weitere Informationen finden Sie im entsprechenden Kapitel des Administratorhandbuchs.
- Sichere Repository-Verbindung. Weitere Informationen finden Sie in Kapitel 9, „Verwenden von SSL zur sicheren Datenübertragung", auf Seite 57.
- FIPS 140-2-Sicherheit und sichere Repository-Datenbankverbindung. Weitere Informationen finden Sie in Kapitel 8, „FIPS 140–2-Konformität", auf Seite 55.
- Single Sign-on. Weitere Informationen finden Sie in Kapitel 6, „Single Sign-on", auf Seite 39.

Vor der Installation

Vor der Installation von IBM SPSS Collaboration and Deployment Services müssen Sie die Ressourcen in Ihrer Umgebung einrichten, damit die Komponenten betrieben werden können. Beispielsweise müssen Sie eine Datenbank für das Content-Repository erstellen und einen Anwendungsserver konfigurieren.

Die folgende Checkliste soll Ihnen als Leitfaden für das Vorgehen vor der Installation dienen:

- Bestimmen Sie den Installationstyp basierend auf der geplanten Systemverwendung und den entsprechenden Systemanforderungen.
- Stellen Sie die Rechner zur Ausführung des Anwendungsservers bzw. der Server-Cluster bereit. Stellen Sie sicher, dass die Server sämtliche Hard- und Softwareanforderungen erfüllen.
- Prüfen Sie die Installation von Benutzerberechtigung und Hostdateisystemberechtigungen.
- Konfigurieren Sie den Anwendungsserver bzw. den Cluster.
- Konfigurieren Sie die Datenbank. Falls erforderlich, migrieren Sie den Inhalt aus der vorherigen Installation mithilfe der Datenbankkopiertools in die neue Datenbank. Weitere Informationen finden Sie in Kapitel 4, „Migration", auf Seite 33.

Planen der Installation

Vor der Installation von IBM SPSS Collaboration and Deployment Services Repository müssen Sie den Installationstyp festlegen, um die Anwendungsumgebung einrichten zu können. IBM SPSS Collaboration and Deployment Services Repository ist ein auf Unternehmen abgestimmtes System, das in eine Vielzahl von Komponenten und Technologien von IBM und anderen Herstellern integriert werden muss. Bei der einfachsten Konfiguration ist eine bereits vorhandene Installation eines Anwendungsservers zum Ausführen der Web-Services erforderlich, die die Funktionalität der Anwendung gewährleisten, sowie eine relationale Datenbank, wie IBM Db2 UDB, Oracle oder Microsoft SQL Server, zum Speichern analytischer Artefakte sowie von Anwendungseinstellungen.

Berücksichtigen Sie beim Planen der Installation folgende Richtlinien:

- In Betriebsumgebungen muss das Repository auf einem System der Serverklasse installiert werden. Weitere Informationen finden Sie im Thema „Hostsystemanforderungen". Die Systemleistung kann durch Ausführen der Repository-Datenbank auf einem separaten, dedizierten Server insgesamt verbessert werden.
- In Unternehmensumgebungen mit hoher Verarbeitungslast (z. B. durch Generieren von Echtzeitscores) und vielen Benutzern empfiehlt sich eine vertikale Skalierung mit einem Anwendungsserver-Cluster statt der Verwendung eines Standalone-Anwendungsservers.
- Das Repository kann zwar zu Ausbildungs- und Demonstrationszwecken auf einem Desktop-Computer oder einem Notebook installiert und ausgeführt werden, es lässt sich auf solchen Systemen jedoch nicht in einer Produktionsumgebung ausführen.

Beim Planen der Bereitstellung von IBM SPSS Collaboration and Deployment Services Repository müssen Sie ferner die zusätzlichen Anforderungen einer Produktionsumgebung berücksichtigen. Um etwa die Verarbeitung analytischer Artefakte und Scoring möglich zu machen, kann es erforderlich sein, dass Ausführungsserver wie IBM SPSS Statistics- und IBM SPSS Modeler-Server eingerichtet werden müssen, für die auch dedizierte Hardware- und Netzressourcen nötig werden können. Zur Aktivierung der E-Mail-Benachrichtigungsfunktion muss ein SMTP-Server verfügbar sein. Außerdem kann es erforderlich sein, die Repository-Authentifizierung über ein externes Verzeichnissystem und Single Sign-on über einen Kerberos-Server zu konfigurieren.

Hostsystemanforderungen

Stellen Sie vor der Installation von IBM SPSS Collaboration and Deployment Services Repository sicher, dass die folgenden Hardware- und Softwareanforderungen erfüllt sind. Bei der Installation mit einem Anwendungsserver-Cluster müssen die Anforderungen bei allen Knoten erfüllt sein.

Informationen zu den aktuellen Systemanforderungen finden Sie in den Berichten zur Kompatibilität von Softwareprodukten auf der Site des IBM Technical Support unter http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html.

Wichtig: Die angegebene Menge an RAM ist der Mindestwert für eine erfolgreiche Installation und Ausführung des Repositorys. Abhängig vom Typ der von IBM SPSS Collaboration and Deployment Services durchgeführten analytischen Verarbeitung können die Anforderungen an den Laufzeitspeicher erheblich größer sein und es kann ein erheblicher Anteil des üblicherweise auf einem System der Serverklasse installierten RAM belegt werden. Beachten Sie, dass für die Installation von Repository-Adaptern für andere IBM SPSS-Produkte, wie beispielsweise dem IBM SPSS Modeler-Adapter, zusätzlicher dedizierter Arbeitsspeicher erforderlich ist. Es wird empfohlen, bei der Abschätzung der Arbeitsspeicheranforderungen für den ausgewählten Anwendungsserver die Dokumentation für den Anwendungsserver zurate zu ziehen.

Bei der Installation in WebSphere muss das mit IBM SPSS Collaboration and Deployment Services verwendete WebSphere-Profil für die Ausführung mit Java 7 SDK oder höher konfiguriert werden. Siehe „WebSphere" auf Seite 12.

Weitere Anforderungen

IBM Installation Manager (für alle Betriebssysteme)

Zur Verwendung eines Repositorys mit Installationsdateien für IBM SPSS Collaboration and Deployment Services muss IBM Installation Manager 1.8.9 oder höher installiert und konfiguriert sein.

Wenn IBM Installation Manager noch nicht im System vorhanden ist, wird das Produkt automatisch installiert, wenn Sie die Installation von IBM SPSS Collaboration and Deployment Services starten. Wenn Sie eine ältere Version von IBM Installation Manager verwenden, müssen Sie das Produkt im Rahmen der Installation aktualisieren.

Wenn IBM Installation Manager nicht automatisch installiert wird und nicht im System vorhanden ist, müssen Sie IBM Installation Manager von der IBM Support-Site (http://www.ibm.com/support) herunterladen und installieren. Informationen zur Speicherposition für den Download und Benutzerinformationen finden Sie in der Dokumentation zu IBM Installation Manager unter http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.

UNIX und Linux

- Für die GUI-basierte Installation von IBM SPSS Collaboration and Deployment Services Repository ist X Window System Terminal-Software erforderlich. Alternativ kann der Server möglicherweise im automatischen Modus ausgeführt werden (Java-Befehlszeilenoption `-Djava.awt.headless=true`) oder das PJA Toolkit (Pure Java AWT) zu verwenden.

Benutzer- und Dateisystemberechtigungen

Als allgemeine Regel sollten Sie das Repository mit denselben Benutzerberechtigungen installieren und konfigurieren, die auch für die Installation und Konfiguration des Anwendungsservers verwendet wurden. Informationen für die Unterstützung von Installationen als Benutzer ohne Rootberechtigung/Verwaltungsaufgaben finden Sie in der Herstellerdokumentation zu Ihrem Anwendungsserver.

Der Benutzer, der das Repository installiert, muss auf dem Hostsystem über die folgenden Berechtigungen verfügen:

- Schreibberechtigung für das Installationsverzeichnis und Unterverzeichnisse.
- Schreibberechtigung für die Bereitstellungs- und Konfigurationsverzeichnisse sowie Lese- und Ausführungsberechtigungen für andere Verzeichnisse des Anwendungsservers.
- Bei Installation des Repositorys mit einem Anwendungsserver-Cluster muss das Repository-Installationsverzeichnis auf dem Host-Computer des Verwaltungsprofils (traditionelles WebSphere-Profil oder Liberty-Profil) freigegeben werden, damit es auf allen Knoten des Clusters verfügbar ist.

Anmerkung: Beim Installieren von IBM SPSS-Inhaltsadaptern müssen Sie denselben Benutzer verwenden, der für die Installation von IBM SPSS Collaboration and Deployment Services Repository verwendet wurde.

Wichtig: Wenn Sie IBM SPSS Collaboration and Deployment Services Repository unter Windows über ein Administratorkonto installieren, müssen Sie alle zugehörigen Dienstprogramme und Scripts, beispielsweise das Konfigurationsdienstprogramm, mit der Administratorberechtigung ausführen.

Virtualisierung

IBM SPSS Collaboration and Deployment Services Repository oder Clientkomponenten können in virtualisierten Umgebungen von anderen Softwareherstellern eingesetzt werden. Beispielsweise kann ein Systemadministrator zur einfacheren Bereitstellung einer Entwicklungs- oder Testumgebung einen virtuellen Server konfigurieren, auf dem IBM SPSS Collaboration and Deployment Services installiert werden soll. Die virtuellen Geräte, die als Hosts für Komponenten von IBM SPSS Collaboration and Deployment Services fungieren, müssen Mindestanforderungen des Systems erfüllen. Weitere Informationen finden Sie im Thema „Hostsystemanforderungen” auf Seite 10.

Vorausgesetzt, die virtualisierte Umgebung erfüllt die Mindestanforderungen des Systems, werden keine Leistungseinbußen für Installationen von IBM SPSS Collaboration and Deployment Services Repository oder der Clients erwartet. Es ist jedoch wichtig anzumerken, dass virtualisierte Systeme verfügbare Ressourcen gemeinsam nutzen können und der Wettstreit um Ressourcen bei einer hohen Verarbeitungslast die Leistung der bereitgestellten Installation von IBM SPSS Collaboration and Deployment Services beeinträchtigen kann.

Beachten Sie, dass zusätzliche Einschränkungen bei der Bereitstellung in virtualisierten Umgebungen bestehen können, wenn der zur Ausführung des Repositorys verwendete Anwendungsserver nicht in diesen Umgebungen bereitgestellt werden kann.

Anwendungsserver

Vor der Installation von IBM SPSS Collaboration and Deployment Services Repository muss ein unterstützter Anwendungsserver oder ein Server-Cluster installiert werden und der Zugriff darauf muss möglich sein.

Sie können entweder den Einzelserver, IBM WebSphere Application Server, der im Lieferumfang von IBM SPSS Collaboration and Deployment Services enthalten ist, oder einen beliebigen anderen unterstützten Anwendungsserver verwenden. Der enthaltene Anwendungsserver ist ausschließlich für die Verwendung mit IBM SPSS Collaboration and Deployment Services Repository lizenziert und kann nicht in einer Clusterumgebung verwendet werden. Weitere Informationen zu IBM WebSphere finden Sie in der Produktdokumentation im IBM Knowledge Center.

Wenn das Repository erneut installiert wird, erstellen Sie den Anwendungsserver erneut, indem Sie beispielsweise ein neues WebSphere-Profil bereitstellen. Stellen Sie sicher, dass die neuesten Versionen der Herstellerpatches auf Anwendungsserverinstallationen angewendet werden. Bei der Installation von IBM SPSS Collaboration and Deployment Services Repository mit einem Anwendungsserver-Cluster müssen alle Clusterknoten dieselbe Version des Anwendungsservers aufweisen und im selben Betriebssystem ausgeführt werden.

Der Anwendungsserver muss mit einer entsprechenden JRE eingerichtet werden. Prüfen Sie, ob Java im 64-Bit-Modus ausgeführt wird und ob Ihr Anwendungsserver im 64-Bit-Modus richtig funktioniert, bevor Sie versuchen, IBM SPSS Collaboration and Deployment Services Repository zu installieren. Wenn Sie beispielsweise JBoss verwenden und JDK sowohl in der 32-Bit-Version als auch in der 64-Bit-Version installiert ist, konfigurieren Sie die JVM für die Ausführung im 64-Bit-Modus, indem Sie die Option `-d64` für den Java-Befehl angeben. Zur Bereitstellung für das WebSphere Liberty-Profil ist IBM JRE in IBM SPSS Collaboration and Deployment Services integriert. Weitere Informationen finden Sie in der Dokumentation des Anbieters des Anwendungsservers.

Wichtig: Zur Unterstützung von Verbindungen über Web-Browser mit inaktivierten Cookies müssen Sie das Umschreiben der URL für Ihren Anwendungsserver aktivieren. In WebSphere beispielsweise ist diese Einstellung in der Administrationskonsole unter **Anwendungsserver** > *Server1* > **Web-Container** > **Sitzungsverwaltung** > **Erneutes Schreiben von URL aktivieren** verfügbar. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Anwendungsserver.

Einschränkung: Das Umschreiben der URL wird von seit früheren Releases nicht mehr verwendeten Features nicht unterstützt. Für diese Features ist möglicherweise die Aktivierung von Cookies erforderlich.

WebSphere

IBM SPSS Collaboration and Deployment Services Repository kann mit einem Standalone-WebSphere-Server, einem verwalteten Server oder einem Cluster ausgeführt werden.

Vor Installation mit einem Standalone-WebSphere-Server

- Erstellen Sie mit der standardmäßigen Anwendungsprofilvorlage ein neues Profil für jede Installation.

Vor Installation mit einem verwalteten WebSphere-Server

- Erstellen Sie das Bereitstellungsverwaltungsprofil.
- Starten Sie das Verwaltungsprofil.
- Erstellen Sie das verwaltete Profil.
- Fügen Sie einen verwalteten Knoten zum Verwaltungsprofil hinzu.
- Erstellen Sie mit der WebSphere-Konsole basierend auf dem verwalteten Knoten den verwalteten Server.

Vor Installation mit einem WebSphere-Cluster

- Erstellen Sie den Cluster und stellen Sie sicher, dass der Zugriff darauf über die Lastausgleichsfunktion möglich ist.

Vor Installation mit einer WebSphere Application Server Network Deployment-Topologie

Erhöhen Sie die Standardspeicherkonfiguration für den WebSphere Deployment Manager-Prozess (**dmgr**) und die WebSphere Nodeagent-Prozesse. Der tatsächliche Speicherbedarf hängt von Ihrem System ab. Eine minimale Speicherkonfiguration würde beispielsweise in der folgenden Erhöhung des Hauptspeichers bestehen:

- Erhöhen Sie für den WebSphere Deployment Manager-Prozess die Mindestgröße des Heapspeichers auf 512 und die maximale Größe des Heapspeichers auf 1024.
- Erhöhen Sie für die WebSphere Nodeagent-Prozesse die Mindestgröße des Heapspeichers auf 256 und die maximale Größe des Heapspeichers auf 512.

Anmerkung: IBM SPSS Collaboration and Deployment Services muss für die Ausführung mit Java 7 SDK oder höher konfiguriert werden. Die neuesten Fixpacks von WebSphere 8.5.5 und WebSphere 9 enthalten bereits Java 8 SDK im Bundle. Java 8 SDK ist die einzige Version, die von WebSphere 9 unterstützt wird. Wenn diese Versionen von WebSphere verwendet werden, ist also keine zusätzliche Konfiguration für Java SDK erforderlich.

Konfigurieren Ihres Profils für die Ausführung mit Java

Anmerkung: Da die neuesten Fixpacks von WebSphere 8.5.5 bereits Java SDK 8 im Bundle enthalten, gilt diese Abschnitt nur für Fixversionen bis WebSphere 8.5.5.8.

Vor der Installation von IBM SPSS Collaboration and Deployment Services in WebSphere muss das mit IBM SPSS Collaboration and Deployment Services verwendete WebSphere-Profil wie folgt für die Ausführung mit Java 7 SDK oder höher konfiguriert werden.

1. Laden Sie **IBM WebSphere SDK Java Technology Edition Version 7.0** herunter und installieren Sie das Produkt in die Installation von WebSphere 8.5.x. Siehe http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.installation.base.doc/ae/tins_installation_jdk7.html.
2. Konfigurieren Sie nach der Installation das WebSphere-Profil für IBM SPSS Collaboration and Deployment Services für die Verwendung des Java 7 SDK. Siehe http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_managesdk.html.
3. WebSphere ermöglicht die globale Konfiguration (alle Profile) des SDK oder die Konfiguration auf der Basis einzelner Profile. So legen Sie Java 7 SDK für ein bestimmtes WebSphere-Profil fest:

   Führen Sie im Verzeichnis `<Anwendungsserver-Stammverzeichnis>/bin` folgende Schritte aus:

   a. Schritt 1: (optional) Zeigen Sie eine Liste der verfügbaren SDK-Namen für die Produktinstallation an (stellen Sie sicher, dass Java 7 SDK vorhanden ist). Beispiel:

```
C:\IBM\WebSphere\AppServer\bin> managesdk -listAvailable
                CWSDK1003I: Verfügbare SDKs:
                CWSDK1005I: SDK-Name: 1.6_64
                CWSDK1005I: SDK-Name: 1.7_64
                CWSDK1001I: Die angeforderte managesdk-Task wurde erfolgreich ausgeführt.
```

b. Schritt 2: Setzen Sie das für IBM SPSS Collaboration and Deployment Services verwendete Profil auf SDK Version 7.0. Beispiel:

```
C:\IBM\WebSphere\AppServer\bin>managesdk -enableProfile -profileName CADS -sdkname 1.7_64 -enableServers
                CWSDK1017I: Das Profil CADS ist jetzt für die Verwendung von SDK 1.7_64 aktiviert.
                CWSDK1001I: Die angeforderte managesdk-Task wurde erfolgreich ausgeführt.
```

Oder gehen Sie wie folgt vor, um Java 7 SDK für alle WebSphere-Profile (und alle erstellten nachfolgenden Profile) festzulegen:

Im folgenden Beispiel wird die Befehlsfolge angezeigt, die Sie verwenden müssen, um die verfügbaren SDKs aufzulisten, das Standard-SDK in SDK Version 7.0 zu ändern und, falls bereits Profile vorhanden sind, die Profile für die Verwendung von SDK Version 7.0 zu aktivieren.

a. Schritt 1: (optional) Zeigen Sie eine Liste der verfügbaren SDK-Namen für die Produktinstallation an (stellen Sie sicher, dass Java 7 SDK vorhanden ist):

```
C:\IBM\WebSphere\AppServer\bin> managesdk -listAvailable
                CWSDK1003I: Verfügbare SDKs:
                CWSDK1005I: SDK-Name: 1.6_64
                CWSDK1005I: SDK-Name: 1.7_64
                CWSDK1001I: Die angeforderte managesdk-Task wurde erfolgreich ausgeführt.
```

b. Schritt 2: Setzen Sie die Befehlsvoreinstellung auf SDK Version 7.0:

```
C:\IBM\WebSphere\AppServer\bin>managesdk -setCommandDefault -sdkname 1.7_64
                CWSDK1021I:Der Standard-SDK-Name für das Profil ist jetzt auf 1.7_64 gesetzt.
                CWSDK1001I: Die angeforderte managesdk-Task wurde erfolgreich ausgeführt.
```

c. Schritt 3: Setzen Sie den Standardwert für neue Profile auf SDK Version 7.0:

```
C:\IBM\WebSphere\AppServer\bin>managesdk -setNewProfileDefault -sdkname 1.7_64
                CWSDK1022I: Für die Erstellung neuer Profile wird jetzt der SDK-Name 1.7_64 verwendet.
                CWSDK1001I: Die angeforderte managesdk-Task wurde erfolgreich ausgeführt.
```

d. Schritt 4: Wenn bereits Profile vorhanden sind, aktivieren Sie die Profile für die Verwendung von SDK Version 7.0:

```
C:\IBM\WebSphere\AppServer\bin>managesdk -enableProfileAll -sdkname 1.7_64 -enableServers
                CWSDK1017I: Das Profil DEPLOYMENT ist jetzt für die Verwendung von SDK 1.7_64 aktiviert.
                CWSDK1001I: Die angeforderte managesdk-Task wurde erfolgreich ausgeführt.
```

Zum Ändern föderierter Profile in einer Network Deployment-Installation muss der Deployment Manager ausgeführt werden. Der Befehl `managesdk` aktualisiert das Masterkonfigurationsrepository. Nach der Ausführung des Befehls muss eine Synchronisationsoperation ausgeführt werden, bevor das neue SDK für die föderierten Profile verwendet werden kann.

JBoss

IBM SPSS Collaboration and Deployment Services Repository kann nur mit einem Standalone-JBoss-Server ausgeführt werden.

Vor Installation mit JBoss

- Erstellen Sie einen neuen Server für jede Repository-Installation.

Anmerkung:

- Es empfiehlt sich, dass nur eine Instanz des Servers ausgeführt wird. Informieren Sie sich in der JBoss-Dokumentation, wenn mehrere Repository-Instanzen auf einem einzelnen Computer eingerichtet werden müssen.
- Der Installationspfad für den JBoss-Anwendungsserver sollte keine Leerzeichen enthalten, wie z. B. in `c:\jboss-eap-6.1` der Fall, um Fehler beim Repository-Start zu vermeiden.

- Wenn Sie JBoss in einer IPv6-Umgebung ausführen, ist eine zusätzliche Konfiguration des Anwendungsservers erforderlich. Weitere Informationen finden Sie in der Red Hat JBoss-Dokumentation.

Liberty

IBM SPSS Collaboration and Deployment Services Repository kann mit einem IBM WebSphere Liberty-Standalone-Server oder -Cluster ausgeführt werden.

Vor Installation mit einem Liberty-Cluster

Erstellen Sie den WebSphere Liberty-Cluster und stellen Sie sicher, dass der Zugriff darauf über die Lastausgleichsfunktion möglich ist.

Datenbank

Vor der Installation von IBM SPSS Collaboration and Deployment Services Repository muss eine Datenbank ausgeführt werden und zugreifbar sein. Zum Einrichten der erforderlichen Steuertabellen und der erforderlichen Infrastruktur ist eine Verbindung zu der Datenbank erforderlich.

Die Datenbank und IBM SPSS Collaboration and Deployment Services Repository müssen nicht auf demselben Server installiert werden, aber einige Konfigurationsdaten sind erforderlich, um die Verbindungsfähigkeit sicherzustellen. Während der Installation werden Sie aufgefordert, den Datenbankservernamen, die Portnummer, den Benutzernamen und das Kennwort sowie den Namen der Datenbank anzugeben, die zum Speichern und Abrufen von Informationen verwendet werden soll.

Wichtig: Sie müssen die Datenbank vor der Installation manuell erstellen. Ein beliebiger gültiger Datenbankname kann verwendet werden, aber wenn keine zuvor erstellte Datenbank vorhanden ist, wird die Installation nicht fortgesetzt.

Datenbankberechtigungen

In der folgenden Tabelle sind die allgemeinen Datenbankberechtigungen angegeben, die ein Benutzer zum Installieren, Aktualisieren und Ausführen von IBM SPSS Collaboration and Deployment Services Repository sowie zum Anwenden von Fixes auf das Produkt benötigt:

Tabelle 2. Benutzerberechtigungen für die Repository-Wartung

Berechtigung	Installation, Anwendung von Fixpacks, Migration	Laufzeit
Beliebiges Schema ändern	Erforderlich	Optional
Funktion erstellen	Erforderlich	Optional
Prozedur erstellen	Erforderlich	Optional
Tabelle erstellen	Erforderlich	Optional
Ansicht erstellen	Erforderlich	Optional
XML-Schemasammlung erstellen	Erforderlich	Optional
Verbinden	Erforderlich	Erforderlich
Löschen	Erforderlich	Erforderlich
Ausführen	Erforderlich	Erforderlich
Einfügen	Erforderlich	Erforderlich
Verweise	Erforderlich	Erforderlich
Auswählen	Erforderlich	Erforderlich
Aktualisieren	Erforderlich	Erforderlich

Wenn Sie beispielsweise das Repository installieren, benötigen Sie alle Berechtigungen in der Tabelle. Nach der Installation können viele der Berechtigungen vor dem Starten und Ausführen des Repositorys entfernt werden. Diese Berechtigungen müssen wiederhergestellt werden, um ein Fixpack anzuwenden.

Die exakten Namen dieser Berechtigungen können je nach Datenbank variieren und es können auch andere Berechtigungen erforderlich sein. In den folgenden Beispielen werden die Berechtigungen für bestimmte Datenbanksysteme veranschaulicht.

Beispiel: Db2 11.1 for Linux, Windows, and UNIX

- BINDADD
- CONNECT
- CREATETAB
- CREATE_EXTERNAL_ROUTINE
- CREATE_NOT_FENCED_ROUTINE
- DATAACCESS
- EXPLAIN
- IMPLICIT_SCHEMA
- DBADM

Anmerkung: DBADM bietet die explizite Berechtigung vom Typ *create schema* (Schema erstellen), die zum Konfiguriren von IBM SPSS Collaboration and Deployment Services Repository erforderlich ist.

Beispiel: Microsoft SQL Server 2016

- ALTER ANY SCHEMA
- CONNECT
- CREATE FUNCTION
- CREATE PROCEDURE
- CREATE TABLE
- CREATE VIEW
- CREATE XML SCHEMA COLLECTION
- DELETE
- EXECUTE
- INSERT
- REFERENCES
- SELECT
- UPDATE

Beispiel: Oracle 12cR1

Die folgenden Berechtigungen sind zum Konfigurieren von IBM SPSS Collaboration and Deployment Services Repository mit der Oracle 12cR1-Datenbank erforderlich:

- CREATE SESSION
- ALTER SESSION
- CREATE TYPE
- CREATE TABLE
- CREATE PROCEDURE
- CREATE VIEW
- CREATE TRIGGER

Die folgenden Berechtigungen sind zum Starten von IBM SPSS Collaboration and Deployment Services Repository mit der Oracle 12c-Datenbank erforderlich:

- `CREATE SESSION`
- `ALTER SESSION`
- `SESSIONS_PER USER` - muss auf einen Wert größer-gleich 100 gesetzt werden.

Db2

Db2 for Linux, UNIX, and Windows

Bei Verwendung einer Datenbank mit Db2 for Linux, UNIX, and Windows reichen die Standardparameter für die Datenbankerstellung nicht aus. Die folgenden zusätzlichen Parameter müssen angegeben werden:

- UTF-8-Zeichensatz
- Pufferpool mit 8-KB-Seiten (im Beispielscript *CDS8K*) für Tabellen mit einer Breite über 4 KB
- 8-KB-Tabellenbereich unter Verwendung des 8-KB-Pufferpools
- 32-KB-Pufferpool (im Beispielscript *CDSTEMP*)
- 32 KB temporärer Tabellenbereich für alle großen Ergebnissets unter Verwendung des 32-KB-Pufferpools

Es folgt ein Beispielscript für die Erstellung einer Datenbank mit dem Namen *SPSSCDS*. Wenn Sie das Script kopieren und einfügen, müssen Sie sicherstellen, dass es, wie dargestellt, genau mit dem SQL-Code übereinstimmt. Beachten Sie, dass das Script auf einen Datenbankdateipfad im UNIX-Format verweist, der bearbeitet werden muss, wenn das Script unter Windows ausgeführt werden soll. Bei Software-Downloads ist das Script im Dokumentationspaket enthalten.

```
CREATE DATABASE SPSSCDS ON /home/cdsuser USING CODESET UTF-8 TERRITORY US COLLATE USING SYSTEM;
CONNECT TO SPSSCDS;
CREATE Bufferpool CDS8K IMMEDIATE SIZE 250 AUTOMATIC PAGESIZE 8 K;
CREATE REGULAR TABLESPACE CDS8K PAGESIZE 8 K MANAGED BY AUTOMATIC STORAGE EXTENTSIZE 8
OVERHEAD 10.5 PREFETCHSIZE 8 TRANSFERRATE 0.14 BUFFERPOOL CDS8K DROPPED TABLE RECOVERY ON;
COMMENT ON TABLESPACE CDS8K IS '';
CREATE Bufferpool CDSTEMP IMMEDIATE SIZE 250 PAGESIZE 32 K;
CREATE SYSTEM TEMPORARY TABLESPACE CDSTEMP PAGESIZE 32 K MANAGED BY AUTOMATIC STORAGE
EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE 0.14 BUFFERPOOL "CDSTEMP";
COMMENT ON TABLESPACE CDSTEMP IS '';
CONNECT RESET;
```

Db2 unter z/OS

- Bei Verwendung der Db2 z/OS-Datenbank müssen Sie sicherstellen, dass das Db2 zOS-Subsystem für Java, gespeicherte Prozeduren, Funktionen und XML aktiviert ist.
- Zur Aktivierung der XQuery-Unterstützung muss PTF UK73139 oder höher angewendet werden.

Konfiguration der JMS-Nachrichtenspeichertabelle

Wenn IBM SPSS Collaboration and Deployment Services Repository mit WebSphere Application Server installiert wird, wird der standardmäßige WebSphere-JMS-Provider, Service Integration Bus (SIB), so konfiguriert, dass er die Repository-Datenbank als JMS-Nachrichtenspeicher verwendet. Wenn das Repository gestartet wird, erstellt es automatisch die erforderlichen JMS-Tabellen in der Datenbank, wenn diese nicht bereits vorhanden sind.

Bei Verwendung von WebSphere unter z/OS mit Db2 müssen Sie die JMS-Nachrichtenspeichertabellen manuell erstellen. Verwenden Sie zur Erstellung der WebSphere-JMS-Nachrichtenspeichertabellen unter z/OS mit Db2 den WebSphere-Befehl *sibDDLGenerator*, um die DDL zu erstellen, und wenden Sie dann die DDL auf die Datenbank an, um die Tabellen zu erstellen. Weitere Informationen zu *sibDDLGenerator* finden Sie in der WebSphere-Dokumentation.

Weitere Überlegungen

Beim Ausführen von Db2 auf dedizierter Hardware empfiehlt es sich, dass Db2 Configuration Advisor für die Verwaltung der Datenbankleistung verwendet wird. Das Erhöhen der Werte für die folgenden Parameter kann die Leistung verbessern:

- **IBMDEFAULTBP**. Die Größe des Pufferpools sollte je nach verfügbarem Speicher festgelegt werden und sich nach den anderen Anwendungen richten, die auf dem System ausgeführt werden.
- **NUM_IOCLEANERS**. Die Anzahl asynchroner Seitenbereinigungen muss mindestens der Anzahl an Prozessoren im System entsprechen.
- **NUM_IOSERVERS**. Durch Erhöhen der Anzahl an E/A-Servern wird das Vorabrufen optimiert.
- **LOCKLIST**. Durch Erhöhen der Speichermenge für die Sperrliste werden bei Schreibvorgängen Zeitlimitüberschreitungen und Deadlocks vermieden.
- **MAXLOCKS**. Der Prozentsatz zu *LOCKLIST*, der erreicht werden muss, bevor der Datenbankmanager eine Eskalation durchführt.

Wenn Db2 auf einem freigegebenen System ausgeführt wird, müssen bei diesen Änderungen die verfügbaren Systemressourcen berücksichtigt werden. Die Db2-Funktionalität zur Selbsteinstellung sollte dabei als Alternative zum Verwalten der Datenbankleistung angesehen werden.

Microsoft SQL Server

Bei Verwendung einer Microsoft SQL Server-Datenbank:

- Das Schema *DBO* muss verwendet werden.
- Zum Konfigurieren des Datenbankzugriffs ist ein SQL Server-Benutzer erforderlich. Windows-basierte Authentifizierung wird nicht unterstützt.
- IP-Adressen müssen für das IP-Netz aktiviert sein.
- Zum Verarbeiten von nicht lateinischen Zeichensätzen müssen entsprechende Optionen verwendet werden. Beispielsweise wird die Verwendung der Kana-sensitiven (_KS) Option zur Unterscheidung der japanischen Hiragana- und Katakana-Zeichen empfohlen. Weitere Informationen zu Datenbankkollation finden Sie in der Microsoft SQL Server-Dokumentation.
- Die ausgewählte Datenbankkollation muss von der Groß-/Kleinschreibung unabhängig (_CI) sein.
- Die Isolation von Momentaufnahmen muss für die Microsoft SQL Server-Datenbank aktiviert sein. Das folgende Beispiel enthält Anweisungen zum Aktivieren der Isolation von Momentaufnahmen:

```
USE MASTER
GO
ALTER DATABASE <Datenbankname> SET ALLOW_SNAPSHOT_ISOLATION ON
GO
ALTER DATABASE <Datenbankname> SET READ_COMMITTED_SNAPSHOT ON
GO
```

Oracle

Initialisierungsparameter

Wenn Sie eine Oracle-Datenbank mit IBM SPSS Collaboration and Deployment Services verwenden, müssen die folgenden Parameter und Konfigurationen verwendet werden. Änderungen erfolgen in den Parameterdateien `init.ora` und `spfile.ora`.

Tabelle 3. Oracle-Datenbankparameter.

Parameter	Einstellung
OPEN_CURSORS	300
NLS_CHARACTERSET	AL32UTF8
NLS_NCHAR_CHARACTERSET	AL16UTF16
SESSIONS_PER USER	Größer-gleich 100

Anmerkung: Setzen Sie beim Erstellen der Oracle-Instanz sowohl NLS_CHARACTERSET als auch NLS_NCHAR_CHARACTERSET.

Tipp: Mithilfe von Parametern wie `NLS_LANG`, `NLS_COMP` oder `NLS_SORT` können Sie die Groß-/Kleinschreibung der Werte für die Benutzeranmeldung für Ihre Oracle-Instanz einstellen. Weitere Informationen zu dem für Ihre Anforderungen am besten geeigneten Parameter finden Sie in der Oracle-Dokumentation.

Oracle XDB

Für eine Oracle-Datenbank muss Oracle XDB (XML-Datenbankfeatures) installiert werden. Sie können dies prüfen, indem Sie eine Abfrage nach dem Schema (Benutzerkonto) **`XDB`** (`SELECT * FROM ALL_USERS`) durchführen oder indem Sie prüfen, ob **`RESOURCE_VIEW`** vorhanden ist (`DESCRIBE RESOURCE_VIEW`). Dem mit IBM SPSS Collaboration and Deployment Services Repository verwendeten Oracle-Principal muss die Rolle **`XDBADMIN`** zugewiesen sein.

Wartung der Repository-Datenbank

Die Datenbank von IBM SPSS Collaboration and Deployment Services Repository sollte unbedingt regelmäßig gewartet werden.

Tabelle 4. Wartungszeitplan für die Repository-Datenbank

Aufgabe	Empfohlener Zeitplan
Sicherung	Täglich
Statistiken aktualisieren	Täglich
Konsistenzprüfung	Wöchentlich
Neu organisieren	Wöchentlich
Neu erstellen	Monatlich

Installation und Konfiguration

Die folgende Checkliste soll Ihnen als Leitfaden für das Vorgehen bei der Installation mit einem Standalone-Anwendungsserver dienen:

- Installieren Sie die Anwendungsdateien auf dem Hostsystem mit IBM Installation Manager.
- Geben Sie in Installation Manager die vorkonfigurierten Anwendungsserver- und Datenbankinformationen ein und konfigurieren Sie dann die Version von IBM SPSS Collaboration and Deployment Services Repository, die mit dem Anwendungsserver und der Datenbank verwendet wird.

Auch wenn sich die Schritte für einen Standalone-Server ebenfalls auf die Installation in einem Cluster beziehen, sind für für die Installation in einer Clustertopologie zusätzliche Schritte erforderlich. Weitere Informationen finden Sie im Thema „Clusterkonfiguration" auf Seite 24.

Installation und Konfiguration

Die Anwendungsdateien von IBM SPSS Collaboration and Deployment Services Repository werden mit IBM Installation Manager auf dem Hostsystem installiert. Die Installationsdateien können über IBM Passport Advantage heruntergeladen werden.

Vom Konfigurationsdienstprogramm von IBM SPSS Collaboration and Deployment Services Repository werden folgende Aufgaben ausgeführt:

- Es werden Datenbankobjekte für das Content-Repository erstellt.
- Es werden Anwendungsserverressourcen wie JMS-Warteschlangen erstellt und Java-Programme auf dem Anwendungsserver bereitgestellt.
- Es werden die Verschlüsselung und die Sicherheit konfiguriert.

Bei einem Standalone-Anwendungsserver ist die Serverkonfiguration der letzte erforderliche Installationsschritt, bei einer Clusterumgebung sind jedoch weitere Schritte erforderlich. Weitere Informationen finden Sie im Thema „Clusterkonfiguration" auf Seite 24.

Vor der Installation und Konfiguration

1. Prüfen Sie, ob der Anwendungsserver installiert wurde und funktioniert. Wenn Sie eine automatische Konfiguration durchführen (eine Konfiguration, die die Artefakte erstellt und für den Anwendungsserver bereitstellt), muss sich der Anwendungsserver in folgendem Zustand befinden:
   - **WebSphere-Standalone-Server:** Der Server muss gestoppt sein.
   - **Verwalteter WebSphere-Server:** Der verwaltete Server muss gestoppt sein. Der Deployment Manager-Server muss ausgeführt werden.
   - **WebSphere-Cluster:** Clustermitglieder müssen gestoppt sein. Der Deployment Manager-Server muss ausgeführt werden.
   - **JBoss:** Der Server muss gestoppt sein.
   - **Liberty-Standalone-Server:** Keine Aktion erforderlich.
   - **Liberty-Cluster:** Der Verbundcontroller und die Clustermitglieder müssen gestoppt werden. Die vom Repository-Server benötigten Funktionen müssen auf dem Controller-Server und Member-Server installiert sein.

     ```
     appSecurity-2.0
     blueprint-1.0
     concurrent-1.0
     ejb-3.2
     ejbLite-3.2
     jaxrs-2.0
     jaxws-2.2
     jca-1.7
     jdbc-4.2
     jms-2.0
     jndi-1.0
     json-1.0
     jsp-2.3
     mdb-3.2
     servlet-3.1
     ssl-1.0
     wab-1.0
     websocket-1.1
     wasJmsClient-2.0
     wasJmsSecurity-1.0
     wasJmsServer-1.0
     transportSecurity-1.0
     javaMail-1.5
     localConnector-1.0
     ejbPersistentTimer-3.2
     jaxb-2.2
     restConnector-2.0
     ```
2. Prüfen Sie, ob der Zugriff auf die Datenbank möglich ist.
3. Wenn Sie eine vorhandene Repository-Datenbank mit WebSphere erneut verwenden, löschen Sie den SIB (JMS-Nachrichtenspeichertabellen).

Installations- und Konfigurationsschritte

1. Melden Sie sich als Benutzer mit den entsprechenden Berechtigungen beim Betriebssystem an. Weitere Informationen finden Sie im Thema „Benutzer- und Dateisystemberechtigungen" auf Seite 11.
2. Starten Sie IBM Installation Manager:

   GUI-Modus:

   ```
   <IBM Installation Manager-Installationsverzeichnis>/eclipse/IBMIM
   ```

   Befehlszeilenmodus:

   ```
   <IBM Installation Manager-Installationsverzeichnis>/eclipse/tools/imcl -c
   ```

3. Wenn das Installationsrepository nicht konfiguriert ist, geben Sie den Repository-Pfad beispielsweise als einen Ort auf dem Hostdateisystem bzw. dem Netz oder als eine HTTP-Adresse an.

   Anmerkung: Damit Sie erfolgreich auf ein Installationsrepository zugreifen können, darf der Pfad der Repository-Position kein Et-Zeichen (&) enthalten.
4. Wählen Sie "IBM SPSS Collaboration and Deployment Services" als zu installierendes Paket aus.

   Anmerkung: Sie können auch Adapter oder Komponenten auswählen, die mit dem Server für IBM SPSS Collaboration and Deployment Services installiert werden, beispielsweise IBM SPSS Collaboration and Deployment Services Scoring Adapter for PMML, vorausgesetzt diese Adapter oder Komponenten sind in den Installationsrepositorys verfügbar.
5. Lesen Sie die Lizenzvereinbarung und akzeptieren Sie deren Bedingungen.
6. Geben Sie die Paketgruppe und das Installationsverzeichnis an.
   - Für die Installation von IBM SPSS Collaboration and Deployment Services Repository ist eine neue Paketgruppe erforderlich.
   - Geben Sie das Installationsverzeichnis für freigegebene Ressourcen an. Sie können das Verzeichnis für gemeinsam genutzte Ressourcen nur bei der ersten Installation eines Pakets angeben.
7. Wählen Sie das **Bereitstellungsziel** aus, indem Sie einen der folgenden Anwendungsservertypen auswählen:
   - Traditionelles WebSphere-Profil
   - WebSphere Liberty-Profil
   - JBoss EAP
8. Geben Sie die Einstellungen für den Anwendungsservertyp an:
   - WebSphere
     - **WebSphere-Profilstammverzeichnis.** Die Verzeichnisposition des WebSphere-Serverprofils. Beachten Sie, dass es sich bei einem verwalteten Server oder Cluster hierbei um den Pfad zum Deployment Manager-Profil handelt.
     - **Stammverzeichnis der WebSphere-Installation.** Die Verzeichnisposition des WebSphere-Servers.
     - **Servertopologie.** Topologie des WebSphere-Profils: Standalone, verwaltet oder Cluster. Sie müssen eine Topologie auswählen, wenn das Deployment Manager-Profil sowohl verwaltete Server als auch Cluster enthält.
     - **URL-Präfix.** Für die Installation in einem Cluster die URL der Lastausgleichsfunktion bzw. des Proxy-Servers für die Weiterleitung der vom Server initiierten Anforderungen.
     - **WebSphere-Server oder -Cluster.** Der Name des WebSphere-Servers oder -Clusters.
     - **WebSphere-Knoten.** Bei einem verwalteten WebSphere-Server der Name des Knotens, auf dem sich der Zielserver befindet. Bei einem WebSphere-Cluster handelt es sich um den Knotennamen des Datenbankmanagerknotens.
     - **JVM.** Die Verzeichnisposition von WebSphere JVM, die vom Zielprofil verwendet wird.
     - **WebSphere-Benutzername und -Kennwort.** Nur, wenn administrative Sicherheit aktiviert ist.
   - JBoss
     - **Pfad zum Serververzeichnis.** Die Verzeichnisposition von JBoss.
     - **JBoss-Server.** Name des JBoss-Servers. Geben Sie den Wert `standalone` an.
     - **JVM.** Die Verzeichnisposition von JBoss-JVM.
     - **URL-Präfix.** Die URL für die Weiterleitung der vom Server initiierten Anforderungen. Das URL-Standardpräfix für JBoss lautet *http://127.0.0.1:8080*, sofern die Servereigenschaften, wie Bindungsadresse oder Port, nicht geändert wurden. Beachten Sie, dass *localhost* nicht als Teil des URL-Präfixes zulässig ist. Wenn externe Clients eine Verbindung mit IBM SPSS Collaboration and Deployment Services Repository herstellen, muss der Wert des Präfixes extern aufgelöst werden können.

- Liberty
  - **Standalone.** Das WebSphere Liberty-Profil ist in den Server für IBM SPSS Collaboration and Deployment Services Repository integriert. Wählen Sie diese Option aus, wenn Sie ein neues Liberty-Profil mit dem Repository-Server installieren möchten.
  - **Cluster.** Wählen Sie diese Option aus, wenn Sie den Server für IBM SPSS Collaboration and Deployment Services Repository in einem vorhandenen Liberty-Cluster installieren möchten.
  - **URL-Präfix.** Nur sichtbar, wenn Sie **Cluster** auswählen. Es handelt sich um die URL für die Weiterleitung der vom Server initiierten Anforderungen. Im Allgemeinen ist sie der Port der Lastausgleichsfunktion für Cluster-Setup.

9. Geben Sie die Verbindungsinformationen für die Datenbank an:
   - **Datenbanktyp.** IBM Db2, SQL Server oder Oracle.
   - **Host.** Der Hostname bzw. die Adresse des Datenbankservers.
   - **Port.** Der Zugriffsport für den Datenbankserver.
   - **Datenbankname.** Der Name der Datenbank, der für das Content-Repository verwendet werden soll.
   - **SID/Servicename.** Für Oracle, SID bzw. Servicename
   - **Als Dienst ausführen.** Für Oracle, gibt an, dass die Verbindung zu einem Datenbankservice hergestellt wurde, anstatt über SID.
   - **Benutzername.** Der Name des Datenbankbenutzers.
   - **Kennwort.** Das Kennwort des Datenbankbenutzers.
10. Geben Sie bei der erneuten Verwendung einer Datenbank aus einer vorherigen Installation an, ob vorhandene Daten beibehalten oder verworfen werden sollen.
11. Geben Sie die Optionen für den Verschlüsselungsschlüsselspeicher an. Der Keystore ist eine verschlüsselte Datei, die den Schlüssel für die Entschlüsselung der vom Repository verwendeten Kennwörter enthält, z. B. das Repository-Administrationskennwort, das Kennwort für den Zugriff auf die Datenbank usw.
    - Geben Sie zur erneuten Verwendung eines Keystores aus einer vorherigen Repository-Installation den Pfad und das Kennwort des Keystores an. Der Schlüssel aus dem alten Keystore wird extrahiert und im neuen Keystore verwendet. Beachten Sie, dass die JRE, die zum Ausführen des Anwendungsservers verwendet wird, mit der JRE kompatibel sein muss, die zum Erstellen der Verschlüsselungsschlüssel verwendet wurde.
    - Wenn Sie keinen bestehenden Keystore wiederverwenden, müssen Sie das Kennwort für den neuen Keystore angeben und bestätigen. Der Keystore wird unter *<Repository-Installationsverzeichnis>/keystore* erstellt.

    Wichtig: Wenn die Keystore-Datei verloren geht, können mit der Anwendung keine Kennwörter mehr entschlüsselt werden, sodass diese nicht mehr verwendet werden kann. Die Keystore-Datei muss anschließend neu installiert werden. Daher ist es empfehlenswert, Sicherungskopien der Keystore-Datei aufzubewahren.
12. Geben Sie den Kennwortwert an, der für die Erstellung des Administratorbenutzerkontos für das integrierte Repository (*admin*) verwendet werden soll. Das Kennwort wird bei der erstmaligen Anmeldung beim Repository verwendet.
13. Wählen Sie den Bereitstellungsmodus aus (automatisch oder manuell):
    - Bei der automatischen Bereitstellung werden Anwendungsserverressourcen erstellt und die Anwendungsdateien bereitgestellt.
    - Bei der manuellen Bereitstellung werden die Anwendungsdatei sowie die Installationsscripts im Ausgabeverzeichnis *toDeploy/<Zeitmarke>* generiert. Diese Artefakte können später zum manuellen Bereitstellen des Repositorys verwendet werden. Die manuelle Konfiguration ist für erfahrene Benutzer vorgesehen, wenn mehr Kontrolle über die Anwendungsserverumgebung erforderlich ist.

14. Prüfen Sie die zusammengefassten Informationen und fahren Sie mit der Installation fort. Wählen Sie im Hauptmenü die Option **Installieren** aus. Die Anwendungsdateien werden im angegebenen Verzeichnis installiert.

- Wenn die Konfiguration erfolgreich durchgeführt wird, können Sie mit den Schritten nach der Installation fortfahren. Hierzu zählen das Starten des Repositorys und das Prüfen der Konnektivität. Weitere Informationen finden Sie im Thema „Nach der Installation" auf Seite 26.
- Wenn Sie den manuellen Bereitstellungsmodus ausgewählt haben, können Sie mit den manuellen Schritten fortfahren. Weitere Informationen finden Sie im Thema Manuelle Bereitstellung.
- Wenn Sie das Repository mit einem Anwendungsserver-Cluster installieren, können Sie mit dem Konfigurieren der anderen Clusterknoten fortfahren. Weitere Informationen finden Sie im Thema „Clusterkonfiguration" auf Seite 24.

Anmerkung: Die Konfiguration kann 15 bis 30 Minuten oder länger dauern (abhängig von Ihrer Hardware, der Netzgeschwindigkeit, der Komplexität der Anwendungsservertopologie usw.). Wenn der Konfigurationsprozess scheinbar nicht mehr reagiert oder wenn ein Fehler gemeldet wird, prüfen Sie die Protokolldateien im Verzeichnis "*<Installationsverzeichnis von IBM SPSS Collaboration and Deployment Services Repository>/log*".

Automatische Konfiguration

Die Konfiguration von IBM SPSS Collaboration and Deployment Services Repository kann automatisiert werden, indem IBM Installation Manager im unbeaufsichtigten Modus mit Eingaben aus einer Antwortdatei von IBM Installation Manager ausgeführt wird. Die Vorlage für die Antwortdatei ähnelt den folgenden Angaben. Beachten Sie, dass diese Vorlage ein Beispiel einer Installation für ein WebSphere Liberty-Profil und eine Db2-Repository-Datenbank ist.

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <variables>
    <variable name='sharedLocation' value='/opt/IBM/IMShared'/>
  </variables>
  <server>
    <repository location=xxxx'/>
    <repository location='xxxx'/>
  </server>
  <profile id='IBM SPSS Collaboration and Deployment Services 8.2' installLocation='/opt/IBM/SPSS/Deployment/8.2/Server'>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='user.LibertyTopologyUserData,com.ibm.spss.cds.server.v8.2.offering' value='single'/>
    <data key='user.KeyPassUserData,com.ibm.spss.cds.server.v8.2.offering' value='xxxx'/>
    <data key='user.ReuseKeyUserData,com.ibm.spss.cds.server.v8.2.offering' value='false'/>
    <data key='user.KeyPwdUserData,com.ibm.spss.cds.server.v8.2.offering' value='xxxx'/>
    <data key='user.AdminPassUserData,com.ibm.spss.cds.server.v8.2.offering' value='xxxx'/>
    <data key='user.AdminPwdUserData,com.ibm.spss.cds.server.v8.2.offering' value='xxxx'/>
    <data key='user.DBPort,com.ibm.spss.cds.server.v8.2.offering' value='50000'/>
    <data key='user.DBName,com.ibm.spss.cds.server.v8.2.offering' value='cadsdb'/>
    <data key='user.DBHost,com.ibm.spss.cds.server.v8.2.offering' value='x.x.x.x'/>
    <data key='user.DBTypeUserData,com.ibm.spss.cds.server.v8.2.offering' value='db2'/>
    <data key='user.DataEraseUserData,com.ibm.spss.cds.server.v8.2.offering' value='false'/>
    <data key='user.DBPassword,com.ibm.spss.cds.server.v8.2.offering' value='xxxx'/>
    <data key='user.SSLServiceUserData,com.ibm.spss.cds.server.v8.2.offering' value='false'/>
    <data key='user.OracleServiceUserData,com.ibm.spss.cds.server.v8.2.offering' value='false'/>
    <data key='user.DBUsername,com.ibm.spss.cds.server.v8.2.offering' value='xxxx'/>
  </profile>
  <install>
    <!-- IBM SPSS Collaboration and Deployment Services - Repository Server 8.2.0.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.2' id='com.ibm.spss.cds.server.v8.2.offering' fea
    <!-- IBM SPSS Modeler Adapters for Collaboration and Deployment Services 18.2.0.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.2' id='com.ibm.spss.modeler.adapter.18.2.0' featu
    <!-- IBM SPSS PMML Scoring Adapter 8.2.0.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.2' id='com.ibm.spss.pmml.scoring.adapter.v8.2' fe
```

```
  </install>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='${sharedLocation}'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='true'/>
</agent-input>
```

So führen Sie die Installation im unbeaufsichtigten Modus aus:

```
<IBM Installation Manager-Installationsverzeichnis>/eclipse/tools/imcl input
responseFile -acceptLicense -showProgress
```

Clusterkonfiguration

IBM SPSS Collaboration and Deployment Services Repository kann in einer Umgebung von in Gruppen zusammengefassten Anwendungsservern bereitgestellt werden. Jeder Anwendungsserver im Cluster sollte die identische Konfiguration für die bereitgestellten Anwendungskomponenten aufweisen und der Zugriff auf das Repository erfolgt durch eine hardware- oder softwarebasierte Lastausgleichsfunktion. Diese Architektur ermöglicht die Verteilung der Verarbeitung auf mehrere Anwendungsserver und bietet Redundanzen für einen etwaigen Ausfall eines Servers.

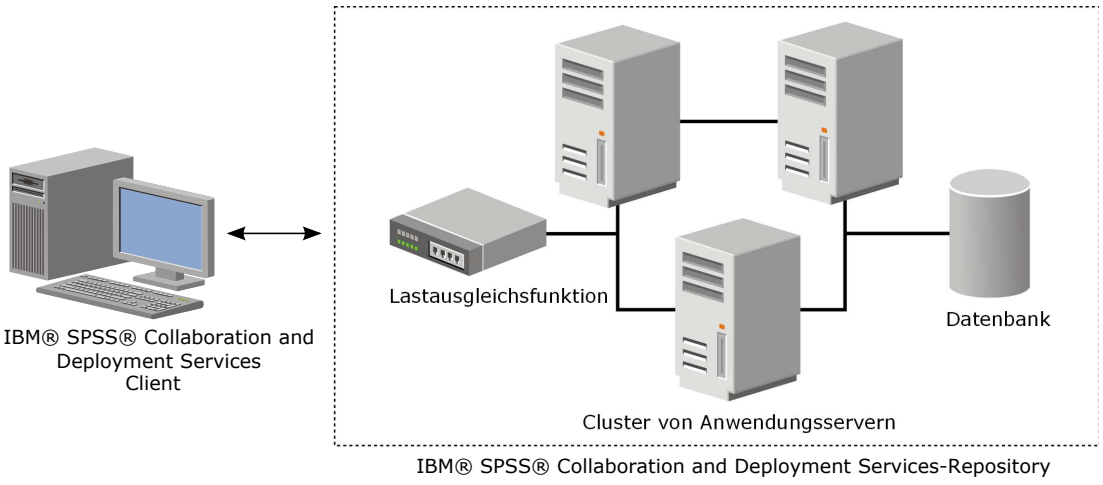

Abbildung 2. Geclusterte Bereitstellungsarchitektur

Der Prozess der Installation des Repositorys in den Cluster beinhaltet folgende Schritte:

- Erstinstallation und -konfiguration von Anwendungskomponenten im Managementknoten des Clusters
- Anschließende Konfiguration von Clusterknoten.

IBM SPSS Collaboration and Deployment Services Repository unterstützt zurzeit das Clustering von traditionellen WebSphere-Anwendungsservernund WebSphere Liberty-Profilen. Führen Sie die Bereitstellung gemäß den Anweisungen für den jeweiligen Anwendungsserver durch.

Installationsvoraussetzungen

- Die Hostsystemanforderungen müssen für alle Knoten des Clusters erfüllt sein.
- Alle Mitglieder des Clusters für IBM SPSS Collaboration and Deployment Services Repository müssen auf demselben Betriebssystem ausgeführt werden wie der Hauptknoten (Managementknoten).
- Die Repository-Datenbank muss bereits bestehen und der Zugriff darauf muss möglich sein.
- Die Topologie des Anwendungsservers muss bereits vor der Installation von IBM SPSS Collaboration and Deployment Services Repository vorhanden sein. Sie sollten vergewissern, dass der Zugriff auf den Cluster sich an der Adresse der Lastausgleichsfunktion möglich ist und dass der Cluster dort ordnungsgemäß ausgeführt wird.
- Das Installationsverzeichnis von IBM SPSS Collaboration and Deployment Services Repository muss für alle Knoten im Cluster freigegeben sein.

WebSphere-Cluster

1. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind.
2. Führen Sie die Installation und Konfiguration durch. Sie können auswählen, ob die Anwendung automatisch oder manuell bereitgestellt werden soll. Weitere Informationen finden Sie im Thema „Installation und Konfiguration" auf Seite 19.
3. Konfigurieren Sie das freizugebende Installationsverzeichnis so, dass alle Mitglieder des Clusters darauf zugreifen können.
4. Legen Sie den Wert der Variablen **CDS_HOME** für die einzelnen Knoten fest.
   - Öffnen Sie die Administrationskonsole.
   - Öffnen Sie den Abschnitt **Umgebung** > **WebSphere-Variablen**.
   - Für jeden Knoten im Cluster ist eine Variable **CDS_HOME** definiert. Prüfen Sie, ob der Wert den entsprechenden Pfad zum freigegebenen Installationsverzeichnis enthält.
5. Legen Sie den Wert der Java-Systemeigenschaft **log4j.configuration** für jedes Clustermitglied fest. Diese Eigenschaft gibt den Speicherort an, an dem das Protokollierungssystem auf die Konfigurationsdatei für die Protokollierung zugreifen kann. Normalerweise hat diese Eigenschaft den folgenden Wert: `file://${CDS_HOME}\platform\log4j.properties`.
   - Öffnen Sie die Administrationskonsole.
   - Prüfen Sie für jeden Server im Cluster den Wert **log4j.configuration**. Dieser Wert ist über **Anwendungsserver** > *Servername* > **Prozessdefinition** > **Java Virtual Machine** > **Benutzerdefinierte Eigenschaften** verfügbar, wobei *Servername* dem jeweiligen Server entspricht.
   - Wenn im Betriebssystem Windows die Variable **CDS_HOME** aus dem Schritt 4 einen Laufwerkbuchstaben enthält, fügen Sie dem Wert **log4j.configuration** als Escapezeichen einen Schrägstrich ("/") hinzu. Der neue Wert würde dann beispielsweise wie folgt lauten: `file:///${CDS_HOME}\platform\log4j.properties`.
6. Speichern und synchronisieren Sie Ihre Änderungen.
7. Stellen Sie sicher, dass der Wert der Konfigurationseigenschaft für das URL-Präfix von IBM SPSS Collaboration and Deployment Services Repository ordnungsgemäß auf die URL der Lastausgleichsfunktion gesetzt ist. Weitere Informationen finden Sie im Thema „Konfiguration der Lastausgleichsfunktion".
8. Starten Sie den Liberty-Cluster.

Konfiguration der Lastausgleichsfunktion

Für den Zugriff auf das Repository in einer Clusterumgebung muss eine software- oder hardwarebasierte Lastausgleichsfunktion konfiguriert werden.

WebSphere-Anwendungsserver enthalten integrierte Dienstprogramme mit einer softwarebasierten Lastausgleichsfunktion (zum Beispiel IBM HTTP Server).

Wichtig: Sitzungsaffinität muss für jede Lastausgleichsfunktion aktiviert sein, die mit dem Cluster für IBM SPSS Collaboration and Deployment Services verwendet wird. Weitere Informationen finden Sie in der Herstellerdokumentation zur Lastausgleichsfunktion.

Einrichten der Eigenschaft "URL-Präfix"

In einer Clusterumgebung muss der Wert der Eigenschaft für das "URL-Präfix" in der Repository-Konfiguration, der für die Weiterleitung der vom Server initiierten HTTP-Anforderungen verwendet wird, auf die URL der Lastausgleichsfunktion gesetzt werden. Beachten Sie, dass diese Eigenschaft erstmals festgelegt werden kann, wenn das Konfigurationsdienstprogramm von IBM SPSS Collaboration and Deployment Services Repository ausgeführt wird. Weitere Informationen finden Sie im Thema Konfiguration.

So können Sie den Wert der Eigenschaft "URL-Präfix" nach der Repository-Konfiguration festlegen/aktualisieren:

- Starten Sie ein einzelnes Clustermitglied.
- Öffnen Sie die browserbasierte Instanz von IBM SPSS Deployment Manager, indem Sie zu *http://<Repository-Host>:<Portnummer>/security/login* navigieren.
- Aktualisieren Sie die Konfigurationseigenschaft *URL_Prefix* mit der URL der Lastausgleichsfunktion für den Cluster und speichern Sie Ihre Änderungen.
- Stoppen Sie das gerade ausgeführte Clustermitglied.
- Starten Sie den Cluster.

Erweitern des Clusters

In Unternehmensumgebungen mit großen Verarbeitungslasten kann es notwendig sein, den Cluster, in dem IBM SPSS Collaboration and Deployment Services Repository ausgeführt wird, zu erweitern, indem nach der ursprünglichen Installation Knoten hinzugefügt werden.

WebSphere

1. Erstellen Sie zusätzliche verwaltete WebSphere-Profile und vereinigen Sie sie in der Zelle. Erstellen Sie Server und fügen Sie sie mithilfe der WebSphere-Konsole zum Cluster hinzu.
2. Führen Sie das Script*CrtCDSresources.py* im Verzeichnis */toDeploy/* aus, um den/die neuen Knoten zu aktualisieren, der/die für die Zelle definiert wurde(n).

   ```
   /bin/wsadmin -lang jython -f CrtCDSresources.py -update
   ```
3. Legen Sie den Wert der Variablen *CDS_HOME* für die einzelnen Knoten fest. Weitere Informationen finden Sie im Thema „WebSphere-Cluster" auf Seite 25.
4. Starten Sie den Cluster neu.

Nach der Installation

Die folgende Checkliste soll Ihnen als Leitfaden für die Schritte nach der Installation dienen:

- Starten Sie den Server und überprüfen Sie die Konnektivität. Konfigurieren Sie gegebenenfalls das automatische Starten des Servers.
- Installieren Sie Inhaltsadapter, um IBM SPSS Collaboration and Deployment Services Repository mit anderen IBM SPSS-Produkten wie IBM SPSS Statistics und IBM SPSS Modeler zu verwenden.
- Installieren Sie bei Bedarf IBM SPSS Collaboration and Deployment Services Remote Process Server und IBM SPSS Collaboration and Deployment Services - Essentials for Python. Weitere Informationen finden Sie in den Installationsanweisungen zu IBM SPSS Collaboration and Deployment Services Remote Process Server 8.2 und IBM SPSS Collaboration and Deployment Services - Essentials for Python 8.2.
- Ändern Sie gegebenenfalls das Master-Datenbankkennwort.
- Installieren Sie gegebenenfalls weitere JDBC-Treiber.
- Installieren Sie IBM SPSS Deployment Manager und Clients für IBM SPSS Collaboration and Deployment Services. Weitere Informationen finden Sie in den Installationsanweisungen der Clientanwendung.
- Erstellen Sie mit Deployment Manager Repository-Benutzer und -Gruppen und weisen Sie über Rollen Anwendungsberechtigungen zu. Weitere Informationen finden Sie im Administratorhandbuch zu IBM SPSS Collaboration and Deployment Services 8.2.

Wenn bei den Schritten nach der Installation Probleme auftreten, informieren Sie sich im Handbuch zur Fehlerbehebung für IBM SPSS Collaboration and Deployment Services 8.2.

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 Dokumentation des Anbieters des Anwendungsservers.

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

Generieren Sie die zugehörigen Konfigurationsdateien, bevor Sie den Repository-Server starten, der in Ihrem WebSphere Liberty-Cluster bereitgestellt wurde. Diese Dateien sind für Liberty für Verbundmember im Cluster erforderlich und sie umfassen die Konfigurationsdateien in `server.xml` in jedem Verbundmember.

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

`<Repository-Installationsverzeichnis>/bin/configUtility.bat`

`<Repository-Installationsverzeichnis>/bin/configUtility.sh`

Geben Sie Werte für Folgendes an:

- **CDS-Ausgangsverzeichnis.** Der Speicherort der IBM SPSS Collaboration and Deployment Services-Systemdateien. Stellen Sie sicher, dass für alle Verbundmember der Zugriff auf diesen Speicherort über Dateifreigabe unter Windows oder NFS unter Linux/UNIX möglich ist.
- **Pfad zum Controller-Member-Server.** Das lokale Verzeichnis des Member-Servers (z. B. `C:\wlp\usr\servers\myController`).
- **Ausgabepfad der generierten Konfigurationsdatei.** Ein gültiger Speicherort im lokalen Dateisystem.

Kopieren Sie alle generierten Konfigurationsdateien in das Verzeichnis, in dem sich `server.xml` auf jedem Member im Cluster befindet. Fügen Sie `server.xml` für jedes Member die folgende Zeile für jede Datei `cads.server.xml` hinzu:

```
<include location="cads.server.xml">
```

Starten Sie dann alle Member im Cluster.

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.

Prüfen der Konnektivität

Sie können prüfen, ob IBM SPSS Collaboration and Deployment Services Repository ausgeführt wird, indem Sie mit einem der folgenden, unterstützten Web-Browser auf die browserbasierte Instanz von IBM SPSS Deployment Manager zugreifen:

- Internet Explorer 10 oder höher
- Firefox 48 ESR oder höher
- Safari 5 oder höher

So greifen Sie auf die browserbasierte Instanz von IBM SPSS Deployment Manager zu:

1. Navigieren Sie zur Anmeldeseite unter *http://<Repository-Host>:<Portnummer>/security/login*.
2. Geben Sie die Anmeldeberechtigungsnachweise des Administrators an. Die Berechtigungsnachweise werden während der Repository-Konfiguration eingerichtet.

Verwalten des Datenbankkennworts

Das bei der Konfiguration von IBM SPSS Collaboration and Deployment Services Repository eingegebene Datenbankkennwort wird als Teil der Datenquellendefinition in den Anwendungsservereinstellungen gespeichert. Es können zusätzliche Schritte erforderlich sein, um die Sicherheit des Datenbankkennworts sicherzustellen.

Testen der Datenbankverbindung

Die Datenbankverbindung von IBM SPSS Collaboration and Deployment Services Repository kann mithilfe der Funktionen zur Datenquellenverwaltung in der Administrationskonsole des Anwendungsservers getestet werden.

Anwendungsserver	Name des Datenquellenobjekts
Traditioneller WebSphere-Server	CDS_DataSource
WebSphere Liberty	CDS_DataSource

Anwendungsserver	Name des Datenquellenobjekts
JBoss	jdbc/spss/PlatformDS

Sicherheit des JAAS-Objekts

Die Berechtigungsnachweise für auf dem Anwendungsserver erstellte Datenquellen von IBM SPSS Collaboration and Deployment Services bleiben als JAAS-Objekt erhalten.

Wichtig: Wird das Repository auf dem WebSphere-Anwendungsserver entweder mithilfe der automatischen Bereitstellung (mit IBM Installation Manager) konfigurieren oder mithilfe der vom Konfigurationsdienstprogramm generierten Scripts konfiguriert, wird das Kennwort als Klartext an den Anwendungsserver weitergegeben und bleibt dann entsprechend der Anwendungsservereinstellungen erhalten. Obwohl die WebSphere-Standardeinstellungen die Speicherung von Kennwörtern in verschlüsselter Form gewährleisten, kann es erforderlich sein, dass Sie sicherstellen, dass das Kennwort nicht als Klartext gespeichert wird. Weitere Informationen zum Kennwortschutz finden Sie in der Anwendungsserverdokumentation.

Ändern des Datenbankkennworts

Aus Sicherheitsgründen kann es erforderlich sein, nach der Installation von IBM SPSS Collaboration and Deployment Services Repository das Datenbankkennwort zu ändern. In diesen Fällen kann das gespeicherte Datenbankkennwort mithilfe des Kennwortdienstprogramms von IBM SPSS Collaboration and Deployment Services geändert werden.

So führen Sie das Kennwortdienstprogramm aus:

1. Beenden Sie den Anwendungsserver, der IBM SPSS Collaboration and Deployment Services bereitstellt.
2. Führen Sie die folgende Datei aus:

   Windows:

   ```
   <Repository-Installationsverzeichnis>/bin/cliUpdateDBPassword.bat
   ```

   UNIX:

   ```
   <Repository-Installationsverzeichnis>/bin/cliUpdateDBPassword.sh
   ```

   System i:

   ```
   <Repository-Installationsverzeichnis>/bin/cliUpdateDBPassword.qsh
   ```
3. Starten Sie den Anwendungsserver, der IBM SPSS Collaboration and Deployment Services bereitstellt.
4. Geben Sie das neue Kennwort an der Eingabeaufforderung ein und bestätigen Sie es.

Das Kennwort kann auch geändert werden, indem Sie die Anwendungsserver-Einstellungen ändern. Beachten Sie, dass das Kennwort in verschlüsselter Form gespeichert wird. Daher kann das neue Kennwort durch Ausführen von `cliEncrypt.bat/cliEncrypt.sh` mit dem Kennwort als Befehlszeilenargument in eine verschlüsselte Zeichenfolge konvertiert werden.

JDBC-Treiber

Hinzufügen der Treiberunterstützung zu IBM SPSS Collaboration and Deployment Services Repository

IBM SPSS Collaboration and Deployment Services umfasst eine Reihe von IBM JDBC-Treibern für alle wichtigen Datenbanksysteme: IBM Db2, Microsoft SQL Server und Oracle. Diese JDBC-Treiber werden standardmäßig zusammen mit dem Repository installiert.

Wenn IBM SPSS Collaboration and Deployment Services keinen Treiber für eine benötigte Datenbank umfasst, können Sie Ihre Umgebung für die Datenbank mit einem Treiber eines anderen Herstellers aktualisieren. Treiber von Drittanbietern können verwendet werden, indem Sie die Repository-Installation mit den Treiberdateien erweitern.

Abhängig vom Anwendungsserver befinden sich die JDBC-Treiber an folgendem Verzeichnisspeicherort:

- WebSphere: `<WebSphere-Installationsverzeichnis>/lib/ext`

Bei JBoss müssen Sie den JDBC-Treiber als JBoss-Kernmodul installieren und das Modul global registrieren. Details finden Sie in der JBoss-Dokumentation.

Beachten Sie, dass für Netezza zum Zugriff auf Datenbanken der Version 4.5 und 5.0 die Treiberversion 5.0 verwendet werden muss.

Hinzufügen der Treiberunterstützung zu Clientanwendungen

So fügen Sie einen JDBC-Treiber zu IBM SPSS Deployment Manager hinzu:

1. Schließen Sie die Clientanwendung, wenn diese ausgeführt wird.
2. Erstellen Sie einen Ordner mit dem Namen `JDBC` auf der Stammverzeichnisebene des Client-Installationsverzeichnisses.
3. Platzieren Sie die Treiberdateien im Ordner `JDBC`.

Nach dem Hinzufügen der Treiberdateien zu Ihrer Umgebung, kann der Treiber in einer Datenquellendefinition verwendet werden. Geben Sie im Dialogfeld "JDBC-Name und URL" den Namen und die URL für den Treiber ein. Informationen zum korrekten Klassennamen und URL-Format des Treibers finden Sie in der Herstellerdokumentation.

Kompatibilität der IBM SPSS-Produkte

Die Funktionen von IBM SPSS Collaboration and Deployment Services Repository können erweitert werden, sodass andere IBM SPSS-Anwendungen durch Installieren zusätzlicher Inhaltsadapterpakete unterstützt werden.

Aktuelle Informationen zur Kompatibilität finden Sie in den Kompatibilitätsberichten zu Softwareprodukten auf der IBM Technical Support-Site unter http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html.

Anmerkung:

- Bei einigen Produkten müssen möglicherweise Patches angewendet werden. Wenden Sie sich an den Support von IBM, um die richtige Patch-Stufe zu ermitteln.
- Sie müssen prüfen, ob die Installations- und Laufzeitanforderungen für IBM SPSS-Anwendungen (z. B. Anwendungsserver und Datenbanken) mit den Anforderungen für IBM SPSS Collaboration and Deployment Services Repository kompatibel sind. Detaillierte Informationen finden Sie in den Kompatibilitätsberichten zu Softwareprodukten sowie in der Dokumentation zu einzelnen IBM SPSS-Produkten.

IBM SPSS Statistics Client und IBM SPSS Modeler Client sind keine Voraussetzung für die Verwendung von IBM SPSS Collaboration and Deployment Services. Diese Anwendungen bieten jedoch Schnittstellen, durch die IBM SPSS Collaboration and Deployment Services Repository verwendet werden kann, um Objekte zu speichern und abzurufen. Die Serverversionen dieser Produkte sind für Jobs erforderlich, die auszuführende IBM SPSS Statistics- oder IBM SPSS Modeler-Objekte enthalten.

Standardmäßig wird das Repository für andere IBM SPSS-Produkte ohne Adapter installiert und die Benutzer müssen die Adapterpakete installieren, die ihren Versionen der Produkte entsprechen. Die Pakete sind auf den Distributionsmedien der Produkte enthalten.

Beachten Sie, dass Sie keine IBM SPSS-Produktobjekte im Repository speichern sollten, bevor Sie die erforderlichen Adapterpakete installiert haben. Andernfalls wird der Objekttyp auch nach der Installation der Adapterpakete nicht erkannt und Sie müssen die Objekte löschen und erneut zum Repository hinzufügen. Wenn beispielsweise ein IBM SPSS Modeler-Datenstrom im Repository gespeichert wird, bevor der IBM SPSS Modeler-Adapter installiert wurde, ist der MIME-Typ nicht bekannt und wird stattdessen auf einen generischen Typ gesetzt, was zu einer unbrauchbaren Datenstromdatei führt.

Deinstallation

Falls eine Installation nicht länger benötigt wird, kann die aktuelle Version deinstalliert werden.

So deinstallieren Sie das Repository:

1. Stoppen Sie das Repository.
2. Wenn bei der Konfiguration des Repositorys die Option "Manuell" verwendet wurde, müssen Sie die Bereitstellung der Repository-Ressourcen aus dem Anwendungsserver zurücknehmen:
   - WebSphere-Standalone-Server

     ```
     <WAS-Profilstammverzeichnis>/bin/wsadmin -lang jython -connType none -f
     <Repository-Installationsverzeichnis>/toDeploy/<Zeitmarke>/delCDS.py
     ```

   - WebSphere, verwalteter Server oder Cluster

     ```
     <WAS-Profilstammverzeichnis>/bin/wsadmin -lang jython -f
     <Repository-Installationsverzeichnis>/toDeploy/<Zeitmarke>/delCDS.py
     ```

   - JBoss

     ```
     <Repository-Installationsverzeichnis>/setup/ant/bin/ant -lib "<Repository-Installationsverzeichnis>/setup/lib"
     -Dinstall.dir="<Repository-Installationsverzeichnis>" -Doutput.dir="."
       -f <Repository-Installationsverzeichnis>/setup/resources/scripts/JBoss/delete-resources.xml
     ```

3. Um alle Daten in der Repository-Datenbank zu löschen, öffnen Sie die Konfigurationsdatei *<Repository-Installationsverzeichnis>/uninstall/uninstall.properties* und setzen Sie `cds.uninstall.remove.user.data property` auf `true` (wahr). Beachten Sie, dass sich einige Daten nach dem Ausführen der Deinstallation von IBM Installation Manager noch immer in der Datenbank befinden können und manuell gelöscht werden müssen.

   Wichtig: Führen Sie diesen Schritt nicht durch, wenn Sie vorhaben, das Repository noch einmal für neue Installationen zu verwenden, oder wenn Sie die Audit- oder Protokolldaten beibehalten müssen. Außerdem sollten Sie in Erwägung ziehen, vor Verwendung dieser Option mithilfe der Tools des Datenbankherstellers eine Datenbanksicherung zu erstellen.
4. Führen Sie IBM Installation Manager (GUI oder Befehlszeile) aus, wählen Sie die Option zur Deinstallation von IBM SPSS Collaboration and Deployment Services aus und folgen Sie den Eingabeaufforderungen. IBM Installation Manager kann auch im unbeaufsichtigten Modus ausgeführt werden. Weitere Informationen finden Sie in der Dokumentation zu IBM Installation Manager unter http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.
5. Löschen Sie manuell das Stamminstallationsverzeichnis des Repositorys.

   Wichtig: Wenn Sie die Wiederverwendung von Repository-Daten planen, sollten Sie die Keystore-Datei unter *<Repository-Installationsverzeichnis>/keystore* speichern.

Kapitel 4. Migration

Bei der Migration von IBM SPSS Collaboration and Deployment Services Repository werden die Inhaltskonfigurationseinstellungen eines bestehenden Repositorys beibehalten. Dazu gehören:

- Dateien und Ordnerstruktur des Repositorys
- Zeitplanungs- und Benachrichtigungskomponenten
- Benachrichtigungsvorlagen
- Lokale Benutzer
- Lokal definierte Ausnahmen der Benutzerlisten und -gruppen für ferne Verzeichnisse
- Rollendefinitionen und Zugehörigkeit
- Benutzervorgaben
- Symbole

Folgende Migrationsszenarios werden unterstützt:

- Migration von einer früheren Version des Repositorys.
- Migration auf einen anderen Host, Anwendungsserver oder Datenbankserver.

Folgende Pfade können für die Migration verwendet werden:

- Installation mit einer Kopie der Repository-Datenbank. Dies ist die empfohlene Migrationsmethode.
- Installation des Repositorys mit einer bestehenden Repository-Datenbank.

Lesen Sie sich vor der Auswahl eines Migrationspfads dieses Kapitel vollständig durch, einschließlich der Informationen unter "Weitere Überlegungen zur Migration".

Unabhängig vom ausgewählten Migrationspfad müssen Sie folgende Richtlinien beachten:

- Anwendungsdateien von IBM SPSS Collaboration and Deployment Services Repository müssen in einem anderen Verzeichnis installiert werden als die ursprüngliche Installation. Überschreiben Sie nicht die Dateien am ursprünglichen Speicherort.
- Eine neue Anwendungsserverinstanz muss erstellt werden. Viederverwenden Sie nicht das Profil (WebSphere) oder den Server (JBoss), das bzw. der bereits zur Ausführung der alten Instanz des Repositorys verwendet wird.
- Beim Migrationsprozess bleibt die Paketkonfiguration des Repositorys nicht erhalten, sodass etwaige zusätzliche Pakete für IBM SPSS-Produkte, beispielsweise IBM SPSS Modeler und IBM SPSS Statistics, erneut installiert werden müssen. Die Pakete in der Zielinstanz müssen sich auf derselben oder auf einer höheren Stufe wie die Pakete im Quellenrepository befinden. Darüberhinaus sollten sie auf die entsprechende Datenbanktabelle verweisen. Die Pakete müssen sich auf einer Stufe befinden, die mit der jeweiligen Zielversion von IBM SPSS Collaboration and Deployment Services kompatibel ist. Weitere Informationen finden Sie im Thema „Kompatibilität der IBM SPSS-Produkte” auf Seite 30.

  Anmerkung: Die Pakete in der Zielinstanz müssen sich auf derselben oder auf einer höheren Stufe wie die Pakete in der Quelleninstanz befinden. Die Informationen zu den installierten Paketen und ihren Versionen finden Sie in der Tabelle `SPSSSETUP_PLUGINS` der Quelleninstanzdatenbank.

Für IBM SPSS Collaboration and Deployment Services 8.2 wird die Migration von Version 8.1.1 unterstützt.

Installation mit einer Kopie der Repository-Datenbank

Bei Verwendung einer Kopie einer bestehenden Repository-Datenbank kann die bestehende Instanz online bleiben, bis die neue Installation bereit für die Aktivierung ist.

Dieses Verfahren dient zur Migration mit einer Kopie der Repository-Datenbank, wobei Quellen- und Zieldatenbank gleich sind, z. B. Db2 auf Db2. Informationen zum Wechseln der Datenbanksysteme finden Sie in „Migration auf eine andere Datenbank"

- Erstellen Sie eine Kopie der bestehenden Repository-Datenbank. Die Datenbankkopie kann mithilfe von Tools des Datenbankanbieters oder von Drittanbietern erstellt werden.
- Führen Sie das Konfigurationsdienstprogramm für IBM SPSS Collaboration and Deployment Services aus und lassen Sie es auf die neue Kopie der Repository-Datenbank verweisen. Achten Sie darauf, dass die Option "Bestehende Daten beibehalten" ausgewählt ist, um alle bestehenden Daten beizubehalten.
- Installieren Sie Zusatzpakete erneut.

Installation mit einer bestehenden Repository-Datenbank

Sie können auch auf IBM SPSS Collaboration and Deployment Services Repository aktualisieren, indem Sie das System mit einer bestehenden Repository-Datenbank installieren.

- Stoppen Sie das Repository.
- Sichern Sie die bestehende Repository-Datenbank.
- Installieren Sie IBM SPSS Collaboration and Deployment Services und führen Sie das Konfigurationsdienstprogramm aus. Achten Sie darauf, dass die Option "Bestehende Daten beibehalten" ausgewählt ist, um alle bestehenden Daten beizubehalten.
- Installieren Sie Zusatzpakete erneut.

Migration auf eine andere Datenbank

Die Migration auf eine andere Datenbank kann einen Wechsel zu einem anderen Datenbankanbieter (beispielsweise von SQL Server zu IBM Db2 oder von Oracle zu Db2) oder die Migration zu einer Datenbank auf einem anderen Betriebssystem beinhalten (beispielsweise von Db2 for i auf Db2 for Linux, UNIX, and Windows).

Repository-Objekte können durch Kopieren der alten Datenbank in die neue Datenbank eines anderen Anbieters übertragen werden.

- Erstellen Sie die Zieldatenbank laut den Anweisungen, die bei der Version von IBM SPSS Collaboration and Deployment Services enthalten waren, die den Ausgangspunkt der Migration bildet.
- Verschieben Sie mithilfe der Tools des Datenbankanbieters die Daten aus der Quellenrepository-Datenbank in die Zielrepository-Datenbank. Die Datenbank sollte bereits konfiguriert sein, sodass die Daten nur noch in die Tabellen von IBM SPSS Collaboration and Deployment Services verschoben werden müssen. Weitere Informationen finden Sie in der Dokumentation des Datenbankherstellers.
- Erstellen Sie eine Kopie der Keystore-Datei, die von der Quellenrepository-Datenbank verwendet wird.
- Installieren Sie IBM SPSS Collaboration and Deployment Services und führen Sie das Konfigurationsdienstprogramm aus.
  - Geben Sie die Zieldatenbank als Repository-Datenbank an.
  - Stellen Sie sicher, dass die Option **Bestehende Daten beibehalten** ausgewählt ist, damit alle bestehenden Daten beibehalten werden.
  - Wenn Sie zur Eingabe des Keystores aufgefordert werden, wählen Sie die Kopie der Keystore-Datei aus, die für die neue Instanz verwendet werden soll.
- Installieren Sie alle Zusatzpakete erneut.

Beachten Sie, dass Sie aufgrund der Unterschiede zwischen Datenbankumgebungen und den Kopiertools der Hersteller, wie Db2-Sicherung, MS SQL Server-Sicherung oder Oracle RMAN, während der Migration sicherstellen müssen, dass die folgenden Datenbankfeatures von dem von Ihnen ausgewählten Tool unterstützt werden:

- XML-Tabellen (*SPSSDMRESPONSE_LOG* und *SPSSSCORE_LOG*)
- Binäre Daten/BLOB, CLOB
- Spezielle Datumsformate

Beispielsweise unterstützt Oracle 12cR1 Data Pump keine XML-Tabellen. Daher kann es zur Wiederherstellung aller Repository-Tabellen mit Ausnahme der beiden XML-Tabellen verwendet werden. Die XML-Tabellen können mit Oracle Export migriert werden. Gehen Sie sämtliche Anforderungen des Datenbankherstellers durch, wie beispielsweise die Registrierung des XML-Schemas in MS SQL Server und Oracle. Es wird empfohlen, dass Sie sich vor der Migration Ihrer Datenbank mit Ihrem Datenbankadministrator besprechen.

Weitere Überlegungen zur Migration

Abhängig von Ihrem Setup können die folgenden zusätzlichen Aufgaben für eine erfolgreiche Migration erforderlich sein:

- Kennwörter
- JMS-Datenspeicher
- Benachrichtigungsvorlagen

Beachten Sie bei der Planung der Migration, dass einige dieser Aufgaben durchgeführt werden müssen, bevor das Konfigurationsdienstprogramm mit einer bestehenden Datenbank oder einer Datenbankkopie ausgeführt wird.

Migration von Kennwörtern

Bei der Migration auf eine neue Instanz von IBM SPSS Collaboration and Deployment Services ist es am besten, eine Java-Umgebung vom selben Anbieter und mit derselben Bit-Größe (32-Bit oder 64-Bit) zu verwenden wie bei der ursprünglichen Installation. Der Grund hierfür ist, dass die im Repository gespeicherten Kennwörter mit einem Keystore-Schlüssel verschlüsselt werden, der von Java Runtime bereitgestellt wird. Für eine andere Java-Bitgröße oder Herstellerimplementierung gilt auch ein anderer Keystore-Schlüssel, mit dem die Kennwörter nicht richtig entschlüsselt werden können. Es kann gelegentlich notwendig sein, den Java-Anbieter zu wechseln bzw. die Bitgröße zu ändern (z. B. beim Wechsel von JBoss zu WebSphere).

Wenn bei der Installation des Repositorys über eine bestehende Datenbank eine andere Java-Verschlüsselung verwendet wird als die, die von der ursprünglichen Instanz verwendet wurde (z. B. IBM Java-Verschlüsselung anstelle von Sun-Java-Verschlüsselung), werden die Kennwörter der Berechtigungsnachweise nicht migriert und das Konfigurationsdienstprogramm meldet einen Fehler. Das Repository kann jedoch trotzdem gestartet werden und Sie können mit IBM SPSS Deployment Manager die Kennwörter der Berechtigungsnachweise manuell ändern. Das Dienstprogramm für den Export/Import migriert Kennwörter, bei erneuter Verwendung einer bestehenden Datenbank muss der Export jedoch von der Quelleninstallation aus durchgeführt werden, bevor die Ressourcen für die Berechtigungsnachweise in die Zielinstallation importiert werden.

Wenn Sie gezwungen sind, eine andere Java-Umgebung zu verwenden, können Sie die Kennwörter in den Ressourcendefinitionen für die Berechtigungsnachweise und in den IBM SPSS Modeler-Jobschritten nach der Konfiguration von IBM SPSS Collaboration and Deployment Services Repository ersetzen:

- Exportieren Sie die Jobs und Ressourcendefinitionen für die Berechtigungsnachweise aus der Instanz des Quellenrepositorys und importieren Sie sie mithilfe von IBM SPSS Deployment Manager in das Zielrepository.

oder

- Aktualisieren Sie die einzelnen Kennwörter in Jobschritten und die einzelnen Berechtigungsnachweise im Zielrepository mithilfe von IBM SPSS Deployment Manager.

Migration des JMS-Speichers unter WebSphere

Wenn IBM SPSS Collaboration and Deployment Services Repository mit WebSphere Application Server installiert wird, wird der standardmäßige WebSphere-JMS-Provider, Service Integration Bus (SIB), so konfiguriert, dass er die Repository-Datenbank als JMS-Nachrichtenspeicher verwendet. Wenn das Repository gestartet wird, erstellt es automatisch die erforderlichen JMS-Tabellen in der Datenbank, wenn diese nicht bereits vorhanden sind. Beachten Sie, dass Sie bei Verwendung von WebSphere unter z/OS mit Db2 die JMS-Nachrichtenspeichertabellen manuell erstellen müssen.

Wenn Sie eine Datenbankkopie verwenden, um den Inhalt eines Repositorys auf eine neue Instanz zu migrieren, die unter WebSphere ausgeführt wird, müssen Sie die JMS-Nachrichtenspeichertabellen (die Tabellen, deren Namen mit "SIB*" beginnen) aus der Datenbank löschen, bevor Sie IBM SPSS Collaboration and Deployment Services starten. Die Tabellen werden dann automatisch erstellt, mit Ausnahme von WebSphere unter z/OS.

Verwenden Sie zur manuellen Erstellung der WebSphere-JMS-Nachrichtenspeichertabellen unter z/OS mit Db2 den WebSphere-Befehl *sibDDLGenerator*, um die DDL zu generieren, und wenden Sie dann die DDL auf die Datenbank an, um die Tabellen zu erstellen. Weitere Informationen zu *sibDDLGenerator* finden Sie in der WebSphere-Dokumentation.

Migration von Benachrichtigungsvorlagen

Um die Anpassungen an Benachrichtigungsvorlagen in einem bestehenden Repository zu erhalten, müssen Sie die Vorlagen unter *<Repository-Installationsverzeichnis>/components/notification/templates* in dasselbe Verzeichnis der neuen Installation kopieren, nachdem die neue Installation erstmals konfiguriert wurde. Weitere Informationen zu Benachrichtigungsvorlagen finden Sie im Administratorhandbuch zu IBM SPSS Collaboration and Deployment Services Repository 8.2.

Kapitel 5. Paketverwaltung

Aktualisierungen, optionale Komponenten und Inhaltsadapter für IBM SPSS-Produkte werden auf dem Server für IBM SPSS Collaboration and Deployment Services Repository als Pakete mit IBM Installation Manager installiert.

Ausführliche Informationen finden Sie in den Installationsanweisungen für die einzelnen Komponenten.

Sie können auch das Dienstprogramm IBM SPSS Collaboration and Deployment Services Package Manager für die Behebung von Problemen mit der Konfiguration von Paketen für IBM SPSS Collaboration and Deployment Services sowie für die Installation zusätzlicher Komponenten, beispielsweise angepasster Inhaltsadapter und Sicherheitsprovider, verwenden.

Installieren von Paketen

IBM SPSS Collaboration and Deployment Services Package Manager ist eine Befehlszeilenanwendung. Das Programm kann auch von anderen Anwendungen im Stapelmodus aufgerufen werden, um deren Paketdateien im Repository zu installieren.

Wenn IBM SPSS Collaboration and Deployment Services Repository ursprünglich automatisch bereitgestellt wurde, muss sich der Anwendungsserver während der Paketinstallation in folgendem Zustand befinden:

- JBoss: Gestoppt
- Liberty: Gestoppt

Der Benutzer muss über Administratorrechte verfügen, damit er Pakete installieren kann.

Damit keine neuere Version eines Pakets mit einer älteren Version überschrieben werden kann, führt Package Manager eine Versionsprüfung durch. Package Manager prüft auch, ob vorausgesetzte Komponenten vorhanden sind, um sicherzustellen, dass sie installiert sind und ihre Versionen gleich oder neuer als die erforderliche Version sind. Die Prüfungen können übergangen werden, beispielsweise um eine ältere Version des Pakets zu installieren.

Anmerkung: Abhängigkeitsprüfungen können nicht überschrieben werden, wenn Package Manager im Stapelmodus aufgerufen wird.

So installieren Sie ein Paket

1. Navigieren Sie zu *<Repository-Installationsverzeichnis>/bin/*.
2. Führen Sie abhängig vom Betriebssystem *cliPackageManager.bat* unter Windows oder *cliPackageManager.sh* unter UNIX aus.
3. Wenn Sie dazu aufgefordert werden, geben Sie Benutzername und Kennwort ein.
4. Geben Sie den Installationsbefehl ein und drücken Sie die `Eingabetaste`. Der Befehl muss die Option `install` und den Pfad des Pakets in Anführungszeichen enthalten, wie in folgendem Beispiel:

   ```
   install 'C:\Verzeichnis 1\Paket1.package'
   ```

   Um mehrere Pakete gleichzeitig zu installieren, geben Sie die Paketnamen durch Leerzeichen getrennt ein, z. B.:

   ```
   install 'C:\Verzeichnis 1\Paket1.package' 'C:\Verzeichis 1\Paket2.package'
   ```

   Alternativ dazu können Sie mehrere Pakete installieren, indem Sie den Parameter `-dir` oder `-d` mit dem Pfad zu einem Verzeichnis verwenden, das die zu installierenden Pakete enthält.

   ```
   install -dir 'C:\CDS-Pakete'
   ```

Bei fehlgeschlagenen Abhängigkeits- bzw. Versionsprüfungen wird wieder die Haupteingabeaufforderung des Package Manager angezeigt. Um nicht schwerwiegende Fehler bei der Installation zu ignorieren, führen Sie den Installationsbefehl mit dem Parameter `-ignore` oder `-i` erneut aus.

5. Wenn die Installation abgeschlossen ist, verwenden Sie den Befehl `exit`, um Package Manager zu schließen.

   Zum Anzeigen weiterer Installationsoptionen der Befehlszeile geben Sie `help` ein und drücken Sie die `Eingabetaste`. Verfügbare Optionen:

   - `info "<Paketpfad>"`: Anzeigen von Information für eine angegebene Paketdatei.
   - `install "<Paketpfad>"`: Installieren der angegebenen Paketdateien im Repository.
   - `tree`: Anzeigen von Hierarchieinformationen für installierte Pakete.

Unbeaufsichtigter Modus

Zur Automatisierung der Paketinstallation kann IBM SPSS Collaboration and Deployment Services Package Manager im unbeaufsichtigten Modus ausgeführt werden:

```
<Repository-Installationsverzeichnis>/bin/cliPackageManager[.sh]
-user <Administrator> -pass <Administratorkennwort>
install <Paketpfad> [<Zusätzlicher_Paketpfad>]
```

Protokollierung

Protokolle von IBM SPSS Collaboration and Deployment Services Package Manager (Hauptprotokoll und Ant-Protokoll) sind unter *<Repository-Installationsverzeichnis>/log* zu finden.

Kapitel 6. Single Sign-on

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.

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

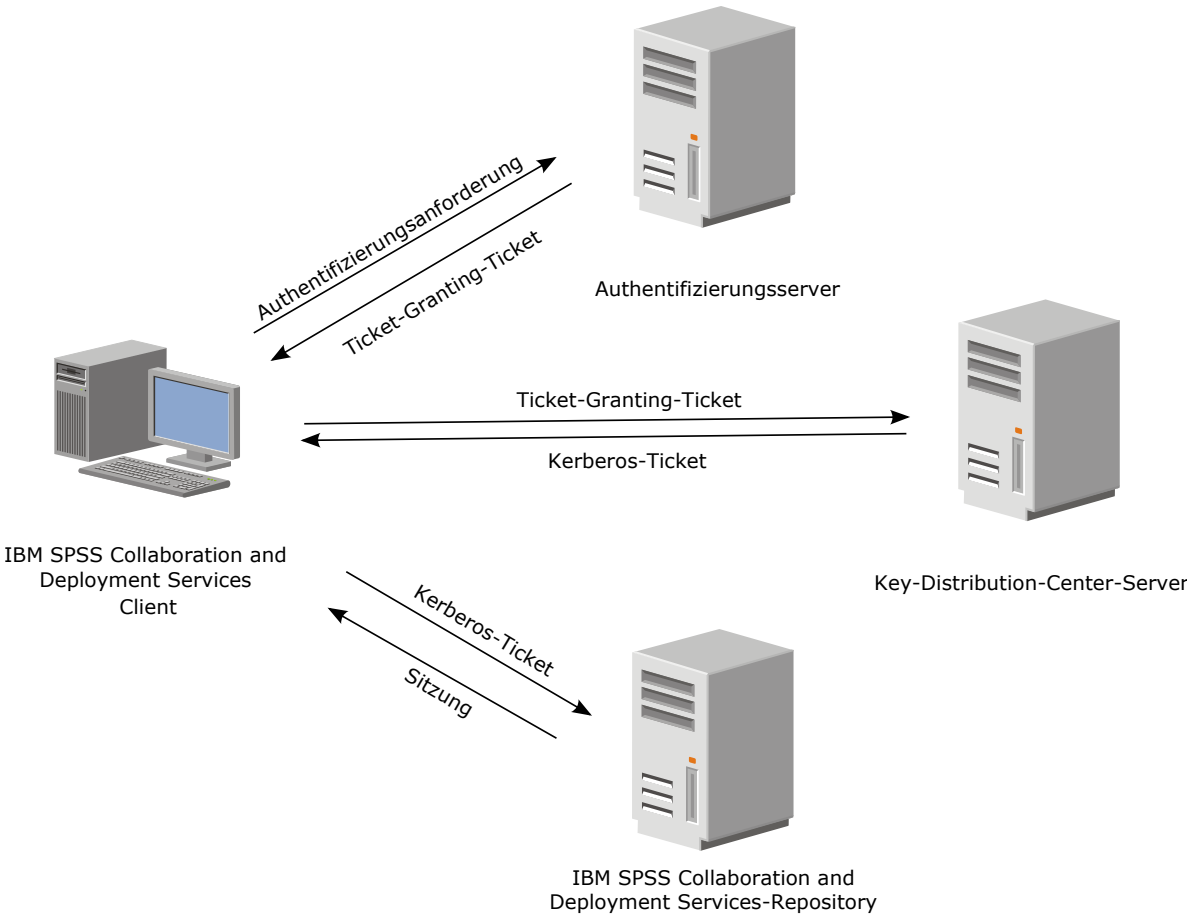

Abbildung 3. SSO-Architektur von IBM SPSS Collaboration and Deployment Services

Wenn beispielsweise IBM SPSS Collaboration and Deployment Services zusammen mit Windows Active Directory verwendet wird, muss für die Aktivierung des Single Sign-on der Kerberos-Service "*Key Distribution Center (KDC)*" konfiguriert werden. Der Service stellt Sitzungstickets und temporäre Sitzungsschlüssel für Benutzer und Computer innerhalb einer Active Directory-Domäne bereit. Der KDC-Service muss auf jedem Domänencontroller als Teil der Active Directory Domain Services (AD DS) ausgeführt werden. Wenn Single Sign-on aktiviert ist, melden sich Anwendungen von IBM SPSS Collaboration and Deployment Services bei einer Kerberos-Domäne an und verwenden Kerberos-Tokens für die Web-Service-Authentifizierung. Falls Single Sign-on aktiviert ist, wird dringend empfohlen, SSL-Kommunikation für das Repository zu konfigurieren.

Desktop-Clientanwendungen wie Deployment Manager erstellen ein Java-Subjekt und stellen dann eine GSS-Sitzung mit dem Repository her, wobei der Kontext des Subjekts verwendet wird. Das Repository gibt ein Kerberos-Service-Ticket an den Client zurück, wenn der GSS-Kontext hergestellt wurde. Thin-Client-Anwendungen wie Deployment Portal beziehen ebenfalls ein Kerberos-Service-Ticket vom Repository. Die Thin-Clients führen jedoch zuerst eine HTTP-basierte plattformübergreifende Authentifizierung über das Negotiate-Protokoll durch. Sowohl Desktop- als auch Thin-Client-Anwendungen machen es erforderlich, dass Sie sich zunächst bei einer Kerberos-Domäne anmelden (z. B. Ihrer Microsoft Active Directory/Windows-Domäne).

Die Konfiguration des Single Sign-on in IBM SPSS Collaboration and Deployment Services umfasst die folgenden Schritte:

- Einrichtung des Verzeichnissystems.
- Konfiguration des Verzeichnissystems als IBM SPSS Collaboration and Deployment Services *Sicherheitsprovider* mit der Registerkarte "Serveradministration" von IBM SPSS Deployment Manager. Weitere Informationen finden Sie in der Administratordokumentation zu IBM SPSS Collaboration and Deployment Services.
- Serverkonfiguration für Kerberos Key Distribution Center. Auf dem Server des Kerberos-Service "Key Distribution Center" muss die Übertragung der Berechtigungsnachweise für den Kerberos-Service-Principal aktiviert sein. Die Vorgehensweise zur Aktivierung der Übertragung der Berechtigungsnachweise unterscheidet sich je nach Ihrem Directory-Server und der Kerberos-Umgebung.
- Konfiguration des Servers von Kerberos Key Distribution Center als Single-Sign-on-Provider für IBM SPSS Collaboration and Deployment Services mit der Registerkarte "Serveradministration" von IBM SPSS Deployment Manager. Weitere Informationen finden Sie in der Administratordokumentation zu IBM SPSS Collaboration and Deployment Services.
- Konfiguration des Anwendungsservers für Single Sign-on.
- Bei Windows-Clientsystemen muss die Registrierung für den Kerberos LSA-Zugriff aktualisiert werden.
- Ja nach dem mit dem Repository verwendeten Anwendungsserver ist es u. U. erforderlich, die Anwendungsserverkonfiguration zu aktualisieren.
- Für Windows-Clientsysteme muss der Registrierungswert `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\` aktualisiert werden. Weitere Informationen finden Sie im Thema „Aktualisieren der Windows-Registrierung für Single Sign-on” auf Seite 44.
- Für den Thin-Client-Zugriff auf das Repository (z. B. mit IBM SPSS Collaboration and Deployment Services Deployment Portal) muss im Web-Browser "Simple and Protected GSS-API Negotiation" (SPNEGO) aktiviert sein.

Außerdem sind weitere Konfigurationsschritte erforderlich, um den Berechtigungsnachweis für die Serverprozesse für das Repository zu aktivieren. Weitere Informationen finden Sie im Thema „Konfiguration von "Berechtigungsnachweis für Serververarbeitung"” auf Seite 46.

Verzeichniskonfiguration für Single Sign-on

Für Single Sign-on von IBM SPSS Collaboration and Deployment Services muss ein externes Verzeichnis eingerichtet werden. Die Directory-Authentifizierung für Single Sign-on von IBM SPSS Collaboration and Deployment Services kann auf den folgenden Verzeichnissystemen basieren:

- OpenLDAP-Verzeichnis
- Microsoft Active Directory

OpenLDAP

Die Gesamtkonfiguration beinhaltet die folgenden Schritte:

- Konfigurieren von OpenLDAP-Sicherheitsprovidern. Weitere Informationen finden Sie im Administratorhandbuch zu IBM SPSS Collaboration and Deployment Services 8.2.

- Kerberos-Server-spezifische Änderungen an der OpenLDAP-Konfiguration, je nach verwendetem Kerberos-Server.

OpenLDAP mit Windows Kerberos Server

Wenn das OpenLDAP-Verzeichnis zusammen mit Windows Kerberos Server verwendet wird, wobei OpenLDAP der Sicherheitsprovider von IBM SPSS Collaboration and Deployment Services und Windows Kerberos Server der Single-Sign-on-Provider (Single Sign-On Provider) ist, müssen Sie sicherstellen, dass Ihr OpenLDAP-Schema mit Ihrem Active Directory-Schema übereinstimmt. Wenn das Schema nicht übereinstimmt, müssen Sie die Benutzerzuordnung beim OpenLDAP-Server ändern.

MIT Kerberos Server

Wenn MIT Kerberos Server zusammen mit OpenLDAP verwendet wird, kann es erforderlich sein, SSL auf dem OpenLDAP-Server und -Client einzurichten, um eine sichere Kommunikation sicherzustellen, wenn sich der KDC-Service und der LDAP-Server auf verschiedenen Hosts befinden. Aktualisierte Informationen finden Sie in der Dokumentation zur jeweiligen Version von MIT Kerberos Server.

Active Directory

Die folgenden Anweisungen wurden für den Windows Server 2003-Domänencontroller erstellt. Die Schritte für Windows Server 2012-Systeme sind ähnlich.

1. Erstellen Sie ein Benutzerprofil, das als Kerberos Service-Principal verwendet werden soll.
2. Ordnen Sie dieses Benutzerprofil dem Hostsystem von IBM SPSS Collaboration and Deployment Services zu.
3. Konfigurieren Sie den Verschlüsselungstyp und die Delegierung der Berechtigungsnachweise für Kerberos.
4. Erstellen Sie eine Kerberos-Chiffrierschlüsseldatei und speichern Sie sie im Hostsystem von IBM SPSS Collaboration and Deployment Services.

Nach Ausführung dieser Schritte können Sie Deployment Manager verwenden, um Active Directory als Sicherheitsprovider zu konfigurieren, und anschließend Kerberos als Single-Sign-on-Provider konfigurieren.

Erstellen eines Benutzerprofils für den Kerberos-Principal

1. Erstellen Sie mithilfe der Active Directory-Benutzer und der Verwaltungskonsole des Computers einen Domänenbenutzer für die ausgewählte Domäne (beispielsweise Benutzer `krb5.principal` in Domäne `spss`). Dieser Benutzer entspricht dem Kerberos-Service-Principal.
2. Geben Sie einen Nachnamenparameter für diesen Benutzer ein. Dieser ist für einige Anwendungsserver erforderlich.
3. Wählen Sie die Option aus, dass das Kennwort nie ablaufen soll.

Zuordnen des Benutzerprofils zum Hostsystem von IBM SPSS Collaboration and Deployment Services

Ordnen Sie das Benutzerprofil mithilfe des Tools **setspn** einem Namen des Service-Principals (SPN – Service Principal Name) zu. Ein SPN ist ein Name, der von einem Kerberos-Client verwendet wird, um einen Service auf einem Kerberos-Server anzugeben. Der Client verweist auf den SPN und nicht auf einen bestimmten Domänenbenutzer.

Das Tool **setspn** greift auf die SPN-Eigenschaft für einen Benutzer zu, aktualisiert und entfernt sie. Verwenden Sie die folgende Befehlssyntax, um einen SPN hinzuzufügen:

```
setspn -A <SPN> <Benutzer>
```

Die Option **-A** fügt dem Domänenkonto einen beliebigen SPN hinzu. Die anderen Argumente weisen folgende Definitionen auf:

<SPN>
Der dem Benutzer hinzugefügte SPN, der folgendes Format aufweist: *<Serviceklasse>/<Host>*. Der Wert *<Serviceklasse>* bezeichnet die Klasse des Service. Der Wert *<Host>* entspricht entweder dem vollständig qualifizierten oder dem einfachen Hostnamen.

<Benutzer>
Das Benutzerprofil, das dem SPN zugeordnet werden soll.

Führen Sie die folgenden Schritte aus, um das Benutzerprofil zuzuordnen. Fügen Sie den vollständig qualifizierten Hostnamen und den einfachen, gekürzten Hostnamen hinzu, da ein Client auf beide Namen verweisen kann.

1. Wenn Sie nicht über das Tool **setspn** verfügen, laden Sie eine geeignete Version der Windows-Support-Tools herunter und installieren Sie sie.
2. Führen Sie **setspn** mit dem vollständig qualifizierten Hostnamen des Servers von IBM SPSS Collaboration and Deployment Services als Argument aus, wie in folgendem Beispiel zu sehen:

   ```
   setspn -A HTTP/cdsserver.spss.com krb5.principal
   ```
3. Führen Sie **setspn** mit dem Hostnamen des Servers von IBM SPSS Collaboration and Deployment Services als Argument aus, wie in folgendem Beispiel zu sehen:

   ```
   setspn -A HTTP/cdsserver krb5.principal
   ```

Weitere Informationen zum Tool **setspn** finden Sie unter http://technet.microsoft.com/en-us/library/cc731241.aspx.

Konfigurieren des Verschlüsselungstyp und der Delegierung der Berechtigungsnachweise für Kerberos

1. Wählen Sie auf der Registerkarte "Konto" des Dialogfelds für die Benutzereigenschaften die Option zur Verwendung von AES-Verschlüsselung aus.
2. Wählen Sie auf der Registerkarte "Delegierung" des Dialogfelds die Option aus, die besagt, dass dem Benutzer bei Delegierungen aller Services vertraut werden soll.

Erstellen einer Kerberos-Chiffrierschlüsseldatei

Eine Chiffrierschlüsseldatei enthält Kerberos-Principals mit ihren entsprechenden verschlüsselten Schlüsseln und wird zur Authentifizierung von Principals verwendet. Mithilfe des Tools **ktpass** können Sie eine Chiffrierschlüsseldatei erstellen. Weitere Informationen zum Tool **ktpass** finden Sie unter http://technet.microsoft.com/en-us/library/cc753771.aspx.

1. Führen Sie das Tool **ktpass** wie im folgenden Beispiel aus:

   ```
   ktpass -out c:\temp\krb5.prin.keytab -princ HTTP/cdsserver.spss.com@SPSS.COM
    -mapUser krb5.principal@SPSS.COM -mapOp set -pass Pass1234 -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL
   ```

   - Der Wert für die Option **princ** muss folgendes Format aufweisen: *<Name_des_Service-Providers>@<Domäne>*.
   - Der Wert für die Option **mapUser** muss das folgende Format aufweisen: *<Kerberos-Service-Principal>@<Domäne>*.
   - Die JCE-Erweiterung für starke Verschlüsselung von Oracle ist für alle Arten der starken Verschlüsselung, wie von der Option **crypto** definiert, erforderlich.
2. Speichern Sie die generierte Chiffrierschlüsseldatei (im Beispiel *C:\temp\krb5.prin.keytab*) im Dateisystem Ihres Hosts für IBM SPSS Collaboration and Deployment Services.

Wenn sich das Servicekennwort ändert, muss die Chiffrierschlüsseldatei aktualisiert werden.

Kerberos-Serverkonfiguration

In Microsoft Windows-Umgebungen wird die Verwendung von Active Directory Server mit (integriertem) Windows-Kerberos-Server empfohlen. Sie müssen die Registrierung aller Client-Computer für Kerberos-LAS-Zugriff aktualisieren. Außerdem müssen Sie bestimmte Änderungen an den Browsern vornehmen, um Kerberos verwenden zu können. Bei Kerberos-Servern, die nicht unter Microsoft Windows ausgeführt werden, müssen Sie möglicherweise zusätzliche Software auf Ihrem Repository-Host-Computer sowie auf den einzelnen Client-Computern installieren. In allen Fällen muss ein Kerberos-Service-Principal zum Delegieren der Berechtigungsnachweise verwendet werden. Außerdem müssen Sie zum Delegieren der Berechtigungsnachweise bestimmte Änderungen an den einzelnen Client-Computern vornehmen.

Konfiguration des Anwendungsservers für Single Sign-on

Abhängig von dem mit dem Repository verwendeten Anwendungsserver müssen Anwendungsservereinstellungen möglicherweise aktualisiert werden.

WebSphere

Die Konfiguration von IBM SPSS Collaboration and Deployment Services für Single Sign-on in WebSphere 7 und 8 umfasst die folgenden Schritte:

- Definieren des Kerberos-Chiffrierschlüssels
- Definieren der JAAS-JGSS-Richtlinie

Definieren des Kerberos-Chiffrierschlüssels

1. Wählen Sie in der Administrationskonsole folgende Optionsfolge aus:

   Server > **Anwendungsserver** > **<Servername>** > **Serverinfrastruktur** > **Prozessdefinition** > **Java Virtual Machine** > **Benutzerdef. Eigenschaften**
2. Fügen Sie die benutzerdefinierte Eigenschaft *KRB5_KTNAME* mit dem Wert des Dateipfads der Chiffrierschlüsseldatei hinzu.

Definieren der JAAS-JGSS-Richtlinie

1. Wählen Sie in der Administrationskonsole folgende Optionsfolge aus:

   Sicherheit > **Sichere Verwaltung, Anwendungen und Infrastruktur** > **Java Authentication and Authorization Service** > **Anwendungsanmeldungen**
2. Definieren Sie die Eigenschaft *JGSSServer*.
3. Definieren Sie in den zusätzlichen Eigenschaften für *JGSSServer* die Modulklasse *com.ibm.security.auth.module.Krb5LoginModule* mit Authentifizierungsstrategie `REQUIRED`.
4. Definieren Sie die folgenden benutzerdefinierten Eigenschaften für *com.ibm.security.auth.module.Krb5LoginModule*.

Eigenschaftsname	**Wert**
credsType	both
principal	<Principal-Name>, z. B. *HTTP/cdsserver.spss.com@SPSS.COM*
useDefaultKeytab	true

JBoss

Für JBoss-Anwendungsserver muss mindestens eine JAAS-Konfiguration (JAAS - Java Authentication and Authorization Service) für JGSSServer angegeben werden. Die Vorlage für eine Single-Sign-on-Anwendungsrichtlinie befindet sich im JGSSServer-Element von `<JBoss-Installationsverzeichnis>/standalone/configuration/standalone.xml` oder `cds_server.xml`. Es kann erforderlich sein, den Namen des Kerberos-Anmeldemoduls so zu ändern, dass es dem Namen der Anwendungsserver-JRE entspricht.

Für JGSSServer muss mindestens eine JAAS-Konfiguration mit folgenden Parametern angegeben werden:

- **JGSSServer** erforderlich
- **KerberosLocalUser** optional
- **JDBC_DRIVER_01** optional

1. Für Sun JRE wird die folgende JGSSServer-Standardkonfiguration erstellt:

```
JGSSServer {
 com.sun.security.auth.module.Krb5LoginModule  required
 storeKey="true"
 doNotPrompt="true"
 realm=<Realmname>
 useKeyTab="true"
 principal=<Name>
 keyTab=<Pfad>
 debug=false;
};
```

2. Die optionale KerberosLocalUser-Konfiguration wird verwendet, um die NTLM-Umgehung zu ermöglichen. Mithilfe dieser Konfiguration kann der Benutzer einen Kerberos-Berechtigungsnachweis erstellen, wenn der Client-Browser während der Negotiation Challenge ein NTLM-Token (anstelle eines Kerberos-Tokens) sendet. Beachten Sie, dass Browser, die auf demselben Rechner wie der Server für IBM SPSS Collaboration and Deployment Services installiert sind, auf Windows-Systemen immer ein NTLM-Token senden. Alle NTLM-Anforderungen an IBM SPSS Collaboration and Deployment Services können inaktiviert werden, indem diese Konfiguration aus ihrer JAAS-Konfigurationsdatei herausgelassen wird.

   Für IBM JRE:

```
KerberosLocalUser {
 com.ibm.security.auth.module.Krb5LoginModule required
 useDefaultCcache=true
 debug=false;
};
```

   Für Sun JRE:

```
KerberosLocalUser {
 com.sun.security.auth.module.Krb5LoginModule  required
 useTicketCache="true"
 debug=false;
};
```

3. Die optionale JDBC_DRIVER_01-Konfiguration wird für die Kerberos-Authentifizierung für Datenbankserver verwendet.

   Für IBM JRE:

```
JDBC_DRIVER_01 {
 com.ibm.security.auth.module.Krb5LoginModule required
 useDefaultCcache=true
 debug=false;
};
```

   Für Sun JRE:

```
JDBC_DRIVER_01 {
 com.sun.security.auth.module.Krb5LoginModule  required
 useTicketCache="true"
 debug=false;
};
```

4. Es ist außerdem möglich, für jede JAAS-Konfiguration einen geeigneten Anmeldemodulklasse nnamen, Anforderungstyp und andere vom Anmeldemodul benötigte Optionen anzugeben. Die Anmeldemodulklasse muss sich im Klassenpfad befinden. Weitere Informationen finden Sie in der Herstellerdokumentation zur JRE und zum Anwendungsserver.

Aktualisieren der Windows-Registrierung für Single Sign-on

Damit SSO ordnungsgemäß funktioniert, muss das Kerberos-Ticket-Granting-Ticket (TGT) den Sitzungsschlüssel enthalten. Die Windows-Registrierung muss aktualisiert werden, damit diese Einbeziehung ermöglicht wird. Weitere Informationen finden Sie unter http://support.microsoft.com/kb/308339.

Die Installationsmedien für IBM SPSS Collaboration and Deployment Services enthalten Registrierungsaktualisierungsdateien zur Konfiguration von Windows XP SP2-, Windows Vista- und Windows 2003-Syste-

men für Kerberos-basiertes Single Sign-on. Die Dateien befinden sich im Verzeichnis /Documentation/Utility_Files/Windows/registry des Dokumentationspakets (von IBM Passport Advantage heruntergeladen). Es handelt sich um folgende Dateien:

- /Server/Kerberos/Win2003_Kerberos.reg
- /Server/Kerberos/WinXPSP2_Kerberos.reg

Verwenden Sie für Windows Vista-Systeme und neuere Systeme die Datei Win2003_Kerberos.reg.

Die Registrierungsdateien gestatten dem Systemadministrator, Registrierungsänderungen auf alle Systeme im Netz zu übertragen, die Single-Sign-on-Zugriff auf das Repository benötigen.

Konfigurieren von unidirektionalen Vertrauensstellungen

Sie können Ihre Umgebung für die realmübergreifende Authentifizierung konfigurieren, um den Benutzerzugriff zu steuern.

Angenommen, Sie haben die zwei Domänen AppDomain und UserDomain. Die beiden Domänen haben eine unidirektionale Vertrauensstellung, wobei AppDomain für die abgehende Vertrauensstellung und UserDomain für die eingehende Vertrauensstellung konfiguriert ist. Sie installieren den Server für IBM SPSS Collaboration and Deployment Services in der Domäne AppDomain und IBM SPSS Deployment Manager in der Domäne UserDomain.

Wenn Sie IBM SPSS Collaboration and Deployment Services für die unidirektionale Vertrauensstellung konfigurieren, müssen Sie sowohl den Server für IBM SPSS Collaboration and Deployment Services als auch IBM SPSS Deployment Manager ändern.

Konfiguration des Servers für IBM SPSS Collaboration and Deployment Services

1. Stoppen Sie den Server für IBM SPSS Collaboration and Deployment Services.
2. Erstellen Sie eine gültige Kerberos-Konfigurationsdatei, krb5.conf, auf dem Serverdateisystem. Der Inhalt der Datei sollte den folgenden Zeilen ähnlich sein, die Domänen sollten jedoch durch die entsprechenden Werte Ihres Systems ersetzt werden:

```
[libdefaults]
default_realm = APPDOMAIN.COM

[realms]
  APPDOMAIN.COM = {
  kdc = kdc.appdomain.com:88
  default_domain = appdomain.com
 }
[domain_realm]
  .appdomain.com = APPDOMAIN.COM
```

3. Setzen Sie die Java-Systemeigenschaft java.security.krb5.conf auf den Speicherort der Datei krb5.conf. Beispiel:

```
-Djava.security.krb5.conf="c:/windows/krb5.conf"
```

   Anweisungen zum Festlegen der Java-Systemeigenschaften finden Sie in der Dokumentation zu Ihrem Anwendungsserver.
4. Starten Sie den Server für IBM SPSS Collaboration and Deployment Services.

Konfiguration von IBM SPSS Deployment Manager

1. Schließen Sie IBM SPSS Deployment Manager.
2. Erstellen Sie im Windows-Installationsordner c:\windows\ eine gültige Kerberos-Konfigurationsdatei, krb5.ini. Der Inhalt der Datei sollte für die realmübergreifende Authentifizierung gültig und den folgenden Zeilen ähnlich sein. Die Domänen sollten jedoch durch die entsprechenden Werte Ihres Systems ersetzt werden:

```
[libdefaults]
default_realm = USERDOMAIN.COM

[realms]
  USERDOMAIN.COM = {
  kdc = kdc.userdomain.com:88
  default_domain = userdomain.com
 }
  APPDOMAIN.COM = {
  kdc = kdc.appdomain.com:88
  default_domain = appdomain.com
 }

[domain_realm]
  .userdomain.com = USERDOMAIN.COM
  .appdomain.com = APPDOMAIN.COM
```

3. Starten Sie IBM SPSS Deployment Manager.

Konfiguration von "Berechtigungsnachweis für Serververarbeitung"

Bei "Berechtigungsnachweis für Serverprozesse" handelt es sich um die integrierte Berechtigungsnachweisdefinition des Benutzerprofils, unter dem der Repository-Server ausgeführt wird. In Active Directory oder in einer auf OpenLDAP beruhenden Single-Sign-on-Umgebung kann der Berechtigungsnachweis für Serverprozesse anstelle der regulären Benutzerberechtigungsnachweise für das Repository verwendet werden, um folgende Aktionen auszuführen:

- Ausführung von Berichtsjobschritten und Planung zeitbasierter Jobs
- Abfrage eines Sicherheitsproviders nach einer Liste mit Benutzer- und Gruppenprofilen

Weitere Informationen zur Verwendung des Berechtigungsnachweises für die Serververarbeitung finden Sie in der Dokumentation zu IBM SPSS Deployment Manager.

Nachdem das Repository für Single Sign-on konfiguriert wurde, sind folgende zusätzliche Schritte zur Aktivierung des Berechtigungsnachweises für die Serververarbeitung erforderlich:

- Konfigurieren Sie die Benutzeranmeldekonfiguration der mittleren Ebene für den Anwendungsserver.
- Erstellen Sie den Kerberos-Ticket-Cache auf dem Repository-Host.

So verwenden Sie den Berechtigungsnachweis für die Serververarbeitung bei Berichtsjobschritten:

- Fügen Sie den Datenbankserver der Datenquelle zur Domäne bzw. zum Realm hinzu.
- Konfigurieren Sie den Datenbankserver der Datenquelle so, dass er Single-Sign-on-Verbindungen von der Domäne/dem Realm akzeptiert.
- Konfigurieren Sie die Datenquellendatenbank so, dass dem Berechtigungsnachweis für die Serververarbeitung die entsprechenden Berechtigungen bereitgestellt werden.

Konfigurieren der Benutzeranmeldekonfiguration der mittleren Ebene bei WebSphere

1. Wählen Sie über die Administrationskonsole Folgendes aus:

   Sicherheit > **Globale Sicherheit** > **JAAS - Anwendungsanmeldungen**
2. Definieren Sie die Anmeldekonfiguration *CaDSMiddleTier*.
3. Definieren Sie für *CaDSMiddleTier* ein JAAS-Modul mit dem Klassennamen *com.ibm.security.auth.module.Krb5LoginModule*.
4. Definieren Sie die folgenden benutzerdefinierten Eigenschaften für *com.ibm.security.auth.module.Krb5LoginModule*:
   - `useDefaultCache` true
   - `renewTGT` true

- debug false

Konfigurieren der Benutzeranmeldekonfiguration der mittleren Ebene bei JBoss

Fügen Sie die folgende Anwendungsrichtlinie zu der Datei *<JBoss-Installationsverzeichnis>/server/<Servername>/conf/login-config.xml* hinzu:

```
<application-policy name="CaDSMiddleTier">
  <authentication>
    <login-module code="com.sun.security.auth.module.Krb5LoginModule" flag="required">
    <module-option name="useTicketCache">true</module-option>
    <module-option name="realm">###DOMAIN#NAME###</module-option>
    <module-option name="kdc">###KDC#SERVER#HOST###</module-option>
    <module-option name="renewTGT">true</module-option>
   </login-module>
  </authentication>
</application-policy>
```

Erstellen des Kerberos-Ticketcache

Der Kerberos-Ticketcache dient zum Speichern des Kerberos-Tickets, mit dem der Berechtigungsnachweis für Serverprozesse authentifiziert wird. Führen Sie zur Erstellung des Ticket-Cache folgende Schritte aus:

1. Aktualisieren Sie die Kerberos-Konfigurationsdatei auf dem Server des Repository-Hosts, z. B. *c:\windows\krb5.ini*. In dieser Datei werden der Standardwert für Realm/Domäne, die Standardcodierungstypen, das erneuerbare Ticket und die KDC-Adresse angegeben und sie wird von der Anwendung **kinit** zur Generierung unseres Ticket-Cache verwendet. Im Folgenden finden Sie ein Beispiel der Kerberos-Konfigurationsdatei:

   ```
   [libdefaults]
     default_realm = ACSSO.COM
     default_tkt_enctypes = rc4-hmac
     default_tgs_enctypes = rc4-hmac
     renewable = true

   [realms]
     ACSSO.COM = {
       kdc = acKDC.ACSSO.COM:88
       default_domain = ACSSO.COM
    }
   ```

2. Melden Sie sich beim Repository-Host mit den Domänenberechtigungsnachweisen an, die als Berechtigungsnachweis für die Serververarbeitung verwendet werden sollen. Stellen Sie sicher, dass diese Berechtigungsnachweise die entsprechenden Berechtigungen für den Host aufweisen.
3. Führen Sie in dem Verzeichnis der JRE, das vom Repository-Anwendungsserver verwendet wird, **kinit** mit den Optionen zur Erstellung eines erneuerbaren Tickets und eines Ticket-Cache aus.

   Anmerkung: Unter Windows-Betriebssystemen erstellt der Befehl **kinit** möglicherweise kein erneuerbares Ticket. Fügen Sie die folgende Registrierungseinstellung hinzu, um dieses Problem zu lösen:

   ```
   \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters\allowtgtsessionkey=0x01
    (DWORD)
   ```

   Weitere Informationen finden Sie in der Kerberos-Dokumentation für Ihr Betriebssystem.
4. Geben Sie das Kennwort für den Benutzer für "Berechtigungsnachweis für Serververarbeitung" ein.

Konfigurieren von Browsern für Single Sign-on

Zur Aktivierung von Single Sign-on für IBM SPSS Collaboration and Deployment Services Deployment Portal und andere Thin-Clients von IBM SPSS Collaboration and Deployment Services müssen Sie Ihren Web-Browser für die Unterstützung des Simple and Protected GSS-API Negotiation-Protokolls (SPNEGO) konfigurieren.

Microsoft Internet Explorer

Informationen zum Konfigurieren von Microsoft Internet Explorer für die Unterstützung von SPNEGO finden Sie unter http://msdn.microsoft.com/en-us/library/ms995329.aspx.

Mozilla Firefox

Die SPNEGO-Unterstützung für Firefox ist standardmäßig inaktiviert. So aktivieren Sie sie:

1. Gehen Sie zur *about:config*-URL (Konfigurationsdateieditor von Firefox).
2. Ändern Sie die folgenden Vorgabewerte:
   - **network.negotiate-auth.allow-non-fqdn** = false
   - **network.negotiate-auth.allow-proxies** = true
   - **network.negotiate-auth.delegation-uris** = Angabe des Domänennamens des lokalen Intranets, beispielsweise .Ihre-Domäne.com, wobei der vorangestellte Punkt ein Platzhalterzeichen darstellt.
   - **network.negotiate-auth.trusted-uris** = Angabe des Domänennamens des lokalen Intranets, beispielsweise .Ihre-Domäne.com, wobei der vorangestellte Punkt ein Platzhalterzeichen darstellt.
   - **network.negotiate-auth.using-native-gsslib** = true

Google Chrome

Die SPNEGO-Unterstützung für Chrome ist standardmäßig inaktiviert. Wenn Sie sie aktivieren wollen, müssen Sie den Namen des Servers für IBM SPSS Collaboration and Deployment Services in einer Whitelist angeben:

- Definieren Sie für Windows die Gruppenrichtlinie AuthNegotiateDelegateWhitelist. Weitere Informationen finden Sie in der Richtlinienliste für Chrome sowie unter dem Problem 472145 und dem Problem 469171.

Als Mitglied der Whitelist wird der Server für IBM SPSS Collaboration and Deployment Services als vertrauenswürdiges Ziel für die Weiterleitung von Kerberos-Tickets behandelt.

Safari

Single Sign-on wird für Safari nicht unterstützt.

Weiterleitbare Tickets und IBM SPSS Deployment Manager

Sie können das Tool **kinit.exe** des JDK verwenden, um Kerberos-Ticket-Granting-Tickets anzufordern und in den Cache zu stellen. Dies ist jedoch nicht erforderlich. Sie können beispielsweise im Verzeichnis jre\bin Ihrer Installation von IBM SPSS Deployment Manager folgenden Befehl absetzen:

```
kinit.exe -f
```

Die Option -f erstellt ein weiterleitbares Ticket. Dieser Befehl erstellt eine Cachedatei im Windows-Verzeichnis Benutzer, in dem die JVM automatisch nach einem Cache sucht.

Wenn Sie diesen Befehl mit einer älteren Version von IBM JDK 7 als 170_SR8 abgesetzt haben, müssen Sie Ihre Datei krb5.ini möglicherweise ändern, damit erfolgreich auf diesen Cache zugegeriffen werden kann.

1. Öffnen Sie die Datei krb5.ini in einem Texteditor. Diese Datei befindet sich häufig im Vereichnis C:\Windows.
2. Fügen Sie im Abschnitt **[libdefaults]:** die folgende Einstellung hinzu:
   ```
   forwardable = true
   ```
3. Speichern Sie die aktualisierte Datei.

Diese Änderung ist nur für den Client erforderlich. Für den Server für IBM SPSS Collaboration and Deployment Services Repository ist keine entsprechende Änderung erforderlich.

Kapitel 7. Kontextstammverzeichnisse der Anwendung

Das Kontextstammverzeichnis einer Anwendung definiert die Position, an der auf das Modul zugegriffen werden kann. Das Kontextstammverzeichnis ist Teil der URL, mit der Sie eine Verbindung zur Anwendung herstellen können.

Eine URL-Referenz auf eine Anwendung von IBM SPSS Collaboration and Deployment Services enthält die folgenden Elemente:

URL-Präfix
Besteht aus dem Protokoll, dem Servernamen oder der IP-Adresse und der Portnummer

Kontextstammverzeichnis
Bestimmt die Position, an der auf die Anwendung zugegriffen wird. Standardmäßig ist das Kontextstammverzeichnis das Serverstammverzeichnis und wird mit einem einzelnen Schrägstrich gekennzeichnet.

Stammverzeichnis der Anwendung
Gibt das Stammverzeichnis der Anwendung an

IBM SPSS Collaboration and Deployment Services Deployment Portal weist beispielsweise die folgende URL auf, wenn der Repository-Server lokal an Port 8080 ausgeführt wird:

```
http://localhost:8080/peb
```

Das URL-Präfix lautet `http://localhost:8080` und das Kontextstammverzeichnis ist das Serverstammverzeichnis der Anwendung. Das Stammverzeichnis der Anwendung lautet `peb`.

Keine Angabe in der URL gibt das Webmodul als Teil von IBM SPSS Collaboration and Deployment Services an. Wenn Sie Ihrem Server andere Anwendungen hinzufügen, wird das Verwalten der zahlreichen, im Serverstammverzeichnis verfügbaren Module zunehmend schwieriger.

Wenn Sie den Repository-Server für die Verwendung eines Kontextstammverzeichnisses konfigurieren, können Sie die Komponenten von IBM SPSS Collaboration and Deployment Services von anderen Anwendungen isolieren. Sie können beispielsweise ein Kontextstammverzeichnis `ibm/spss` für die Module von IBM SPSS Collaboration and Deployment Services definieren. In diesem Fall lautet die URL für die Schnittstelle von IBM SPSS Collaboration and Deployment Services Deployment Portal wie folgt:

```
http://localhost:8080/ibm/spss/peb
```

Wichtig: Wenn Sie für Ihren Repository-Server ein Kontextstammverzeichnis verwenden, müssen alle Clientanwendungen beim Herstellen der Verbindung zum Server dasselbe Kontextstammverzeichnis enthalten. Die URL für Anwendungen, die in der Umgebung von IBM SPSS Collaboration and Deployment Services, beispielsweise IBM Analytical Decision Management, ausgeführt werden, muss entsprechend aktualisiert werden.

Konfigurieren der Kontextstammverzeichnisse der Anwendung

Sie müssen das URL-Präfix des Systems aktualisieren und die einzelnen Spezifikationen des Kontextstammverzeichnisses zum Konfigurieren von Kontextstammverzeichnissen ändern.

Vorgehensweise

1. Wenn die Verwendung eines URL-Präfixes aktiviert ist, fügen Sie dem URL-Präfix das Kontextstammverzeichnis hinzu.

2. Aktualisieren Sie das Kontextstammverzeichnis für jede Anwendung. Die Schritte sind abhängig vom Anwendungsserver.
   - „Aktualisieren der Kontextstammverzeichnisse für WebSphere"
   - „Aktualisieren von Kontextstammverzeichnissen für JBoss" auf Seite 53

Ergebnisse

Sie können mithilfe der URL-Werte, die Ihr Kontextstammverzeichnis enthalten, auf die browserbasierte Instanz von IBM SPSS Deployment Manager und auf IBM SPSS Collaboration and Deployment Services Deployment Portal zugreifen.

Nächste Schritte

Aktualisieren Sie Referenzen auf den Repository-Server, wie z. B. die mit IBM SPSS Deployment Manager definierten Referenzen, um das Kontextstammverzeichnis in die Server-URL einzuschließen.

Hinzufügen eines Kontextstammverzeichnisses zum URL-Präfix

Wenn Ihr System ein benutzerdefiniertes URL-Präfix für den Zugriff auf IBM SPSS Collaboration and Deployment Services Repository verwendet, fügen Sie das Kontextstammverzeichnis der Spezifikation des URL-Präfixes hinzu.

Vorbereitende Schritte

- Ihre Berechtigungsnachweise für die Anmeldung müssen der Konfigurationsaktion zugeordnet sein.
- Die Verwendung der Einstellung für das URL-Präfix muss mithilfe der browserbasierten Instanz von IBM SPSS Deployment Manager aktiviert werden.

Vorgehensweise

1. Melden Sie sich an der browserbasierten Instanz von IBM SPSS Deployment Manager an.
2. Klicken Sie im Fenster **Konfiguration** auf die Option **URL-Präfix** in der Gruppe **Setup**.
3. Fügen Sie das Kontextstammverzeichnis der Definition **URL-Präfix** hinzu. Wenn Ihr URL-Präfix beispielsweise `http://myserver:8080` lautet und Sie das Kontextstammverzeichnis `ibm/spss` verwenden möchten, lautet der neue Wert `http://myserver:8080/ibm/spss`.

   Einschränkung: Beenden Sie die URL-Angabe nicht mit einem Schrägstrich. Beispielsweise müssen Sie `http://server:8080/root` statt `http://server:8080/root/` angeben.
4. Starten Sie den Anwendungsserver neu.

Nächste Schritte

Aktualisieren Sie das Kontextstammverzeichnis für jede Anwendung. Die Schritte sind abhängig vom Anwendungsserver.

Aktualisieren der Kontextstammverzeichnisse für WebSphere

Ändern Sie mithilfe der Administrationskonsole die Position, an der auf unter WebSphere bereitgestellte Anwendungen zugegriffen wird.

Vorbereitende Schritte

„Hinzufügen eines Kontextstammverzeichnisses zum URL-Präfix"

Vorgehensweise

1. Melden Sie sich an der WebSphere-Konsole an.
2. Greifen Sie auf die Anwendung von IBM SPSS Collaboration and Deployment Services zu.
3. Aktualisieren Sie die Einstellungen für das Kontextstammverzeichnis für Webmodule, um den Stammwert einzuschließen. Wenn das URL-Präfix für Ihr System aktiviert ist, muss der Stammwert der einzelnen Module mit dem Wert übereinstimmen, den Sie dem URL-Präfix hinzugefügt haben. Das Stammverzeichnis der Anwendung darf nicht geändert werden. Beispiel: /IBM/SPSS/CDS/admin
4. Starten Sie die WebSphere-Knoten erneut, auf denen IBM SPSS Collaboration and Deployment Services bereitgestellt ist.

Aktualisieren von Kontextstammverzeichnissen für JBoss

Ändern Sie die Position, an der auf unter JBoss bereitgestellte Anwendungen zugegriffen wird, indem Sie die EAR-Datei aktualisieren, die die Positionsdefinitionen enthält.

Vorbereitende Schritte

„Hinzufügen eines Kontextstammverzeichnisses zum URL-Präfix" auf Seite 52

Vorgehensweise

1. Erstellen Sie eine Sicherungskopie der Datei `cds80.ear` im Verzeichnis `toDeploy/timestamp` Ihrer JBoss-Installation.
2. Verwenden Sie ein Archivierungsdienstprogramm, um die Datei `META-INF/application.xml` in der ursprünglichen EAR-Datei zu ändern. Verwenden Sie das neue Kontextstammverzeichnis als Präfix für den Stammverzeichniswert der Anwendung für jedes `context-root`-Element. Sie müssen jedem `context-root`-Element denselben Wert hinzufügen.
3. Kopieren Sie die EAR-Datei, die die aktualisierte Datei `application.xml` enthält, in das Verzeichnis `deploy` des Anwendungsservers.
4. Starten Sie den Anwendungsserver neu.

Beispiel

Angenommen, die Datei `application.xml` enthält die folgenden Spezifikationen:

```
<module>
   <web>
     <web-uri>admin.war</web-uri>
     <context-root>admin</context-root>
   </web>
</module>
<module>
   <web>
     <web-uri>peb.war</web-uri>
     <context-root>peb</context-root>
   </web>
</module>
```

Um das Kontextstammverzeichnis `ibm/spss` hinzuzufügen, aktualisieren Sie die `context-root`-Definitionen mit den folgenden Werten:

```
<module>
   <web>
     <web-uri>admin.war</web-uri>
     <context-root>ibm/spss/admin</context-root>
   </web>
</module>
<module>
   <web>
```

```
      <web-uri>peb.war</web-uri>
      <context-root>ibm/spss/peb</context-root>
    </web>
</module>
```

Kapitel 8. FIPS 140–2-Konformität

Die Federal Information Processing Standard (FIPS) Publication 140-2, FIPS PUB 140-2, ist ein von der US-Bundesregierung festgelegter Computersicherheitsstandard, der zur Anerkennung kryptografischer Module verwendet wird. In diesem Dokument sind die Anforderungen an Kryptografie-Module aufgeführt, die sowohl Hardware- als auch Softwarekomponenten betreffen und vier verschiedenen Sicherheitsstufen entsprechen, die für Unternehmen, die mit der US-Regierung in Geschäftsbeziehungen stehen, obligatorisch sind. IBM SPSS Collaboration and Deployment Services kann für die Bereitstellung von Sicherheitsebene 1 konfiguriert werden, wie durch FIPS 140-2 angegeben.

Bei der Sicherheitskonfiguration müssen folgende Richtlinien eingehalten werden, um eine Übereinstimmung mit FIPS 140-2 zu gewährleisten:

- Die Kommunikation zwischen dem Repository und Clientanwendungen muss über SSL erfolgen, um die Sicherheit der Transportebene bei allgemeinen Datenübertragungen zu gewährleisten. Für Anmeldekennwörter steht zusätzlich AES-Verschlüsselung zur Verfügung, die einen freigegebenen Schlüssel verwendet, der im Code der Anwendung gespeichert ist. Weitere Informationen finden Sie in Kapitel 9, „Verwenden von SSL zur sicheren Datenübertragung", auf Seite 57.
- Der Repository-Server verwendet den AES-Algorithmus, wobei der Schlüssel in einem Keystore im Dateisystem des Servers gespeichert ist, um Kennwörter in Konfigurationsdateien, Anwendungsserverkonfigurationsdateien, Sicherheitsproviderkonfigurationsdateien usw. zu verschlüsseln.
- Für die Kommunikation zwischen dem Repository-Server und dem Datenbankserver kann optional SSL verwendet werden, um die Sicherheit der Transportebene bei allgemeinen Datenübertragungen zu gewährleisten. Für Anmeldekennwörter, Konfigurationskennwörter, Kennwörter für Benutzervorgaben usw. steht AES-Verschlüsselung zur Verfügung, wobei ein freigegebener Schlüssel verwendet wird, der in einem Keystore im Dateisystem des Datenbankservers gespeichert ist.

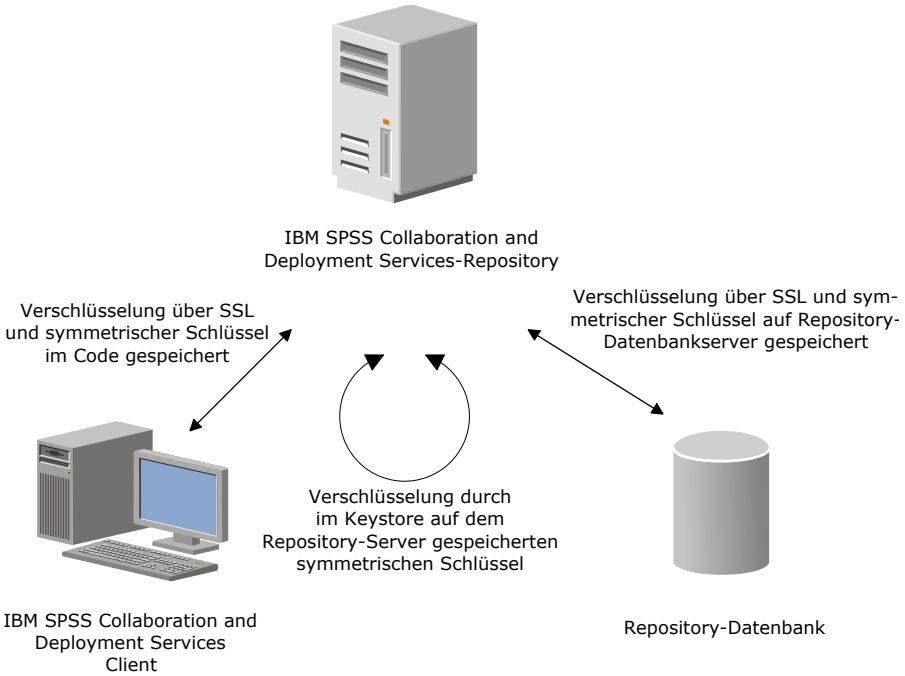

Abbildung 4. Sicherheitssetup von IBM SPSS Collaboration and Deployment Services in Übereinstimmung mit FIPS 140-2

Repository-Konfiguration

Bei der Konfiguration des Repository müssen folgende Richtlinien einhalten werden, um eine Übereinstimmung mit FIPS 140-2 zu gewährleisten:

- Die Datenbank muss so eingerichtet werden, dass sie SSL-Kommunikation akzeptiert; außerdem muss das JCE-Verschlüsselungsmodul konfiguriert werden.
- Wenn das Repository unter UNIX installiert wird, muss die Standard-JRE mit einem JCE-Modul eingerichtet werden.
- Die Anwendungsserver-JRE muss ebenfalls mit einem JCE-Modul eingerichtet werden.
- Der Anwendungsserver muss so konfiguriert werden, dass er SSL-Kommunikation akzeptiert; außerdem muss ein JCE-Modul konfiguriert werden.
- Wenn das Repository unter Windows installiert wird, müssen Sie die Installation im Setup-Fenster beenden, ein JCE-Modul konfigurieren, danach das Setup erneut starten und im entsprechenden Fenster für die Ausführung den Modus in Übereinstimung mit FIPS 140-2 auswählen.
- Wenn das Repository in einer Clusterumgebung bereitgestellt wird, muss der Keystore für alle Knoten im Cluster reproduziert werden.
- Für die JREs, die von IBM Serveranwendungen in Interaktion mit IBM SPSS Collaboration and Deployment Services genutzt werden, z. B. IBM SPSS Statistics Server und IBM SPSS Modeler Server, müssen SSL-Zertifikate installiert sein.

Desktop-Client-Konfiguration

Bei IBM SPSS Collaboration and Deployment Services Desktop-Clientanwendungen wie IBM SPSS Deployment Manager muss das JCE-Verschlüsselungsmodul für die JRE aktiviert werden, die für die Ausführung der Anwendungen verwendet wird. Für die JRE müssen SSL-Zertifikate installiert sein.

Browserkonfiguration

- Mozilla Firefox kann für die Ausführung im FIPS 140-2-konformen Modus konfiguriert werden, in dem die Anwendungsoptionen geändert werden. Weitere Informationen finden Sie unter http://support-.mozilla.com/en-US/kb/Configuring+Firefox+for+FIPS+140-2.
- Die Konfiguration für Internet Explorer erfordert die Aktivierung der Windows-Verschlüsselung und eine Änderung der Browsereinstellungen. Weitere Informationen finden Sie unter http://support.microsoft.com/kb/811833.
- Apple Safari kann im FIPS 140-2-konformen Modus nicht verwendet werden.

Kapitel 9. Verwenden von SSL zur sicheren Datenübertragung

Secure Sockets Layer (SSL) ist ein Protokoll für die Verschlüsselung von Daten, die zwischen zwei Computern übertragen werden. SSL sorgt dafür, dass die Kommunikation zwischen den Computern sicher ist. SSL kann die Authentifizierung von Benutzername/Kennwort sowie den Inhalt eines Austauschs zwischen einem Server und einem Client verschlüsseln.

Funktionsweise von SSL

SSL beruht auf dem öffentlichen und privaten Schlüssel des Servers sowie einem Public-Key-Zertifikat, das die Identität des Servers mit seinem öffentlichen Schlüssel verbindet.

1. Wenn ein Client eine Verbindung zu einem Server aufbaut, authentifiziert der Client den Server mit dem Public-Key-Zertifikat.
2. Der Client generiert dann eine Zufallszahl, verschlüsselt die Zahl mit dem öffentlichen Schlüssel des Servers und sendet die verschlüsselte Nachricht zurück an den Server.
3. Der Server entschlüsselt die Zufallszahl mit seinem privaten Schlüssel.
4. Aus der Zufallszahl generieren Server und Client die Sitzungsschlüssel, die zur Verschlüsselung und Entschlüsselung nachfolgender Informationen verwendet werden.

Das Public-Key-Zertifikat ist in der Regel von einer Zertifizierungsstelle signiert. Zertifizierungsstellen wie VeriSign und Thawte sind Organisationen, die Sicherheitsdaten, die sich in den Public-Key-Zertifikaten befinden, herausgeben, authentifizieren und verwalten. Im Wesentlichen bestätigt die Zertifizierungsstelle die Identität des Servers. Die Zertifizierungsstelle berechnet gewöhnlich eine Gebühr für ein Zertifikat, jedoch können auch selbstsignierte Zertifikate generiert werden.

IBM SPSS Statistics Server unterstützt OpenSSL und GSKit. Wenn beides konfiguriert ist, wird standardmäßig GSKit verwendet.

Schützen der Client/Server- und Server/Server-Kommunikation durch SSL

Hauptschritte beim Schützen der Client/Server- und Server/Client-Kommunikation durch SSL:

1. Beziehen und installieren Sie das SSL-Zertifikat und die Schlüssel.
2. Bei Verwendung von Verschlüsselungszertifikaten mit einer Stärke von mehr als 2048 Bit installieren Sie auf den Deployment Manager-Client-Computern Verschlüsselung mit unbegrenzter Stärke. Weitere Informationen finden Sie in „Installieren der Verschlüsselung mit unbegrenzter Stärke".
3. Fügen Sie das Zertifikat zum Client-Keystore hinzu.
4. Weisen Sie Benutzer an, bei der Verbindung zum Server SSL zu aktivieren.

Anmerkung: Gelegentlich fungiert ein Serverprodukt als Client. Ein Beispiel ist ein IBM SPSS Statistics-Server, der eine Verbindung zum IBM SPSS Collaboration and Deployment Services Repository aufbaut. In diesem Fall ist IBM SPSS Statistics-Server der *Client*.

Installieren der Verschlüsselung mit unbegrenzter Stärke

Bei der als Teil des Produkts ausgelieferten Java Runtime Environment ist Verschlüsselung mit US-Exportstärke aktiviert. Zur besseren Sicherheit Ihrer Daten wird ein Upgrade auf eine Verschlüsselung mit unbegrenzter Stärke empfohlen.

IBM J9

1. Laden Sie JCE-Standortrichtliniendateien (JCE - Java Cryptography Extension) mit unbegrenzter Stärke für Ihre Version des SDK von der Website IBM.com herunter.
2. Extrahieren Sie die in der komprimierten Datei gepackten Standortrichtliniendateien mit unbegrenzter Stärke. Die komprimierte Datei enthält eine Datei namens `US_export_policy.jar` und eine Datei namens `local_policy.jar`. Wechseln Sie in Ihrer Installation von WebSphere Application Server zum Verzeichnis `$JAVA_HOME/jre/lib/security` und erstellen Sie eine Sicherungskopie der Dateien `US_export_policy.jar` und `local_policy.jar`.
3. Ersetzen Sie die vorhandenen Dateien *US_export_policy.jar* und *local_policy.jar* durch die beiden Dateien, die Sie heruntergeladen und extrahiert haben.

   Anmerkung: Sie müssen zudem die `*.jar`-Dateien in Ihrem Ordner `<Deployment-Manager-Clientinstallation>/jre/lib/security` installieren.
4. Aktivieren Sie die Sicherheit in der Administrationskonsole von WebSphere Application Server. Stellen Sie vorab sicher, dass alle Knotenagenten in der Zelle aktiv sind. Weitere Informationen finden Sie in der WebSphere-Dokumentation. Beachten Sie, dass Sie eine verfügbare Realmdefinition aus der Liste unter **Sicherheit > Sichere Verwaltung, Anwendungen und Infrastruktur** auswählen müssen, und klicken Sie dann auf **Als aktuell festlegen**, sodass die Sicherheit bei einem Serverneustart aktiviert wird.
5. Melden Sie sich bei der Administrationskonsole ab.
6. Stoppen Sie den Server.
7. Starten Sie den Server neu.

Sun Java

1. Laden Sie die JCE-Standortrichtliniendateien (JCE - Java Cryptography Extension) mit unbegrenzter Stärke für Ihre Version des SDK von der Sun Java-Website herunter.
2. Extrahieren Sie die heruntergeladene Datei.
3. Kopieren Sie die beiden JAR-Dateien *local_policy.jar* und *US_export_policy.jar* in das Verzeichnis *<Installationsordner>/jre/lib/security*, wobei *<Installationsordner>* der Ordner ist, in dem Sie das Produkt installiert haben.

Hinzufügen des Zertifikats zum Client-Keystore (für Verbindungen zum Repository)

Anmerkung: Überspringen Sie diesen Schritt, wenn Sie ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert wurde.

Wenn Sie SSL für die Verbindung zu einem Repository von IBM SPSS Collaboration and Deployment Services verwenden und außerdem selbstsignierte Zertifikate verwenden, müssen Sie das Zertifikat dem Java-Keystore des Clients hinzufügen. Die folgenden Schritte werden am *Client*-Computer ausgeführt.

1. Öffnen Sie eine Eingabeaufforderung und wechseln Sie in folgendes Verzeichnis, wobei *<Produktinstallationsverzeichnis>* das Verzeichnis ist, in dem Sie das Produkt installiert haben:

   ```
   <Produktinstallationsverzeichnis>/jre/bin
   ```
2. Geben Sie folgenden Befehl ein:

   ```
   keytool -import -alias <Aliasname> -file <Pfad zum Zertifikat> -keystore <Pfad zum Keystore>
   ```

   Dabei ist *<Aliasname>* ein beliebiger Aliasname für das Zertifikat, *<Pfad zum Zertifikat>* ist der vollständige Pfad zum Zertifikat und *<Pfad zum Keystore>* ist der vollständige Pfad zum Java-Keystore, der *<Produktinstallationsverzeichnis>/lib/security/jssecacerts* oder *<Produktinstallationsverzeichnis>/lib/security/cacerts* sein kann.
3. Wenn Sie dazu aufgefordert werden, geben Sie das Keystore-Kennwort ein (standardmäßig `changeit`).

4. Wenn Sie gefragt werden, ob dem Zertifikat vertraut werden soll, geben Sie `yes` (Ja) ein.

Importieren der Zertifikatsdatei für browserbasierte Clientverbindungen

Wenn Sie die Verbindung zu IBM SPSS Collaboration and Deployment Services Repository über SSL mit einem browserbasierten Client, beispielsweise IBM SPSS Collaboration and Deployment Services Deployment Portal, aufbauen, fordert Sie der Browser entweder zum Akzeptieren des nicht signierten, nicht vertrauenswürdigen Zertifikats auf oder zeigt eine Nachricht an, dass die Site nicht sicher ist und bietet einen Link zum Importieren des Zertifikats in den Truststore des Browsers an. Dieser Prozess ist je nach Browser unterschiedlich und kann auch je nach Browserkonfiguration unterschiedlich sein. Sie können das Zertifikat auch manuell im Truststore des Browsers installieren.

Anweisung an Benutzer, SSL zu aktivieren

Wenn Benutzer durch ein Clientprodukt eine Verbindung zum Server aufbauen, müssen Sie SSL im Dialogfeld für die Verbindung zum Server aktivieren. Fordern Sie Ihre Benutzer unbedingt auf, das korrekte Kontrollkästchen zu markieren.

Konfiguration des URL-Präfixes

Wenn IBM SPSS Collaboration and Deployment Services Repository für SSL-Zugriff eingerichtet wird, muss die Einstellung der URL-Präfixkonfiguration wie folgt geändert werden:

1. Melden Sie sich beim Repository mit der browserbasierten Konsole an.
2. Öffnen Sie die Konfigurationsoption *URL-Präfix*.

   Konfiguration > **Setup** > **URL-Präfix**
3. Stellen Sie den Wert des Präfix auf `https` anstelle von `http` ein und setzen Sie den Portwert auf die SSL-Portnummer. Beispiel:

```
[default]
http://<Hostname>:<Port>
[SSL-enabled]
https://<Hostname>:<SSL-Port>
```

Schützen von LDAP mit SSL

Lightweight Directory Access Protocol (LDAP) ist ein IETF-Standard (Internet Engineering Task Force) für den Informationsaustausch zwischen Netzverzeichnissen und Datenbanken mit jedem Informationsgehalt. Für Systeme, die zusätzliche Sicherheit benötigen, können LDAP-Anbieter wie Microsofts Active Directory über Secure Socket Layer (SSL) betrieben werden, vorausgesetzt der Web- oder Anwendungsserver unterstützt LDAP über SSL. Die Verwendung von SSL in Kombination mit LDAP kann sicherstellen, dass Anmeldekennwörter, Anwendungsdaten und andere vertrauliche Daten nicht gefährdet, abgefangen oder gestohlen werden.

Das folgende Beispiel illustriert, wie LDAPS mithilfe von Microsoft Active Directory als Sicherheitsanbieter aktiviert wird. Genauere Informationen zu jedem dieser Schritte oder Details zu einem bestimmten Release des Sicherheitsproviders finden Sie in der entsprechenden Herstellerdokumentation.

1. Stellen Sie sicher, dass Active Directory und die Unternehmenszertifizierungsstelle installiert sind und funktionieren.
2. Generieren Sie mithilfe der Zertifizierungsstelle ein Zertifikat und importieren Sie dieses Zertifikat in den Zertifikatspeicher der Installation von IBM SPSS Deployment Manager. Dies ermöglicht, dass eine LDAPS-Verbindung zwischen IBM SPSS Collaboration and Deployment Services Repository und einem Active Directory-Server aufgebaut wird.

   Um IBM SPSS Deployment Manager für sichere Active Directory-Verbindungen zu konfigurieren, stellen Sie sicher, dass eine Verbindung zum Repository besteht.
3. Starten Sie IBM SPSS Deployment Manager.
4. Wählen Sie **Serververwaltung** im Menü **Extras** aus.

5. Melden Sie sich bei einem zuvor definierten verwalteten Server an.
6. Doppelklicken Sie auf das Symbol **Konfiguration** für den Server, um die Hierarchie zu erweitern.
7. Doppelklicken Sie auf das Symbol **Sicherheitsanbieter**, um die Hierarchie zu erweitern.
8. Doppelklicken Sie auf den Active Directory-Sicherheitsanbieter.
9. Geben Sie Konfigurationswerte für die Active Directory-Instanz mit installierten Sicherheitszertifikaten ein.
10. Markieren Sie das Kontrollkästchen **SSL verwenden**.
11. Geben Sie den Namen im Feld "Domänenbenutzer" an. Nachfolgende Anmeldungen mit Active Directory werden mit SSL authentifiziert.

Weitere Informationen zum Installieren, Konfigurieren und Implementieren von LDAPS auf einem bestimmten Anwendungsserver finden Sie in der entsprechenden Herstellerdokumentation.

Kapitel 10. Protokollierung

Protokollierung ist für die Behebung von Anwendungsproblemen sowie für die Planung präventiver Wartungsaktivitäten von grundlegender Bedeutung. Administratives Personal kann im Zuge der Erstellung von System- und Anwendungsereignissen benachrichtigt werden, wenn Schwellenwerte erreicht werden oder kritische Systemereignisse auftreten. Außerdem können umfangreiche Informationsausgaben in einer Textdatei gespeichert werden, wodurch eine spätere Analyse ermöglicht wird.

IBM SPSS Collaboration and Deployment Services Repository verwendet das log4j-Paket zur Handhabung der Informationen aus dem Laufzeitprotokoll. Log4j ist die Protokolllösung der Apache Software Foundation für Java-Anwendungen. Die Methode log4j ermöglicht die Steuerung der Protokollierung über eine Konfigurationsdatei; die Binärdatei der Anwendung muss dabei nicht verändert werden. Umfangreiche Informationen zu log4j finden Sie auf der log4j-Website.

Konfigurationsdatei für die Protokollierung

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`

In dieser Datei sind sowohl der Speicherort als auch der Umfang der Protokollausgabe festgelegt. Die Konfiguration von log4j wird über eine Anpassung dieser Datei vorgenommen, bei der Appender für das Protokollziel definiert und die Ausgabe der Protokollfunktion an diese Appender geleitet wird.

Folgende Standardprotokollfunktionen sind definiert:

Tabelle 5. Protokollfunktionen.

Protokollfunktion	Beschreibung
log4j.rootCategory	Stammprotokollfunktion
log4j.logger.com.spss	Alle Ereignisse von IBM SPSS Collaboration and Deployment Services
log4j.com.spss.cmor, *log4j.com.spss.cmor.internal.MetaObjectImportEngine*	Repository-Ereignisse
log4j.com.spss.security	Sicherheitsereignisse
log4j.com.spss.process	Jobplanungsereignisse
log4j.com.spss.reporting, *log4j.com.spss.reportservice*	Berichterstellung über Ereignisse
log4j.com.spss.notification	Benachrichtigungsereignisse
log4j.logger.org.springframework.jdbc.core.JdbcTemplate	Spring Framework-JDBC-Ereignisse
log4j.logger.com.spss.repository.internal.transfer	Export-Import-Ereignisse

Die folgenden Appender sind definiert:

- Konsole
- Hauptprotokoll (*cds.log*)
- Protokoll der Export-/Importtransaktionen (*cds_transfer.log*)

Der Standardspeicherort der Protokolldateien variiert abhängig vom Hostanwendungsserver:

- **WebSphere:** <*WebSphere-Profilverzeichnis*>/logs/
- **JBoss:** <*JBoss-Serververzeichnis*>/log/

Kapitel 11. Beispiel: WebSphere-Clusterinstallation und -konfiguration

In diesem Abschnitt wird ein umfassendes Beispiel für das Installieren und Konfigurieren von IBM SPSS Collaboration and Deployment Services Repository mit einem IBM WebSphere-Cluster-Server bereitgestellt.

Im folgenden Beispiel werden die folgenden Informationen schrittweise dargelegt:

- **Schritte vor der Installation** zum Ermitteln der Systemanforderungen basierend auf dem Installationstyp und der Systemverwendung, zum Bereitstellen der Computer für die Ausführung des Clusters von Anwendungsservern und zum Sicherstellen der Einhaltung aller Hardware- und Softwareanforderungen durch die Server.
- **WebSphere-Cluster-Server-Schritte** zum Installieren von WebSphere mit IBM Installation Manager und Einrichten eines WebSphere-Cluster-Servers.
- **Datenbankschritte** zum Initialisieren Ihrer Datenbank.
- **Installations- und Konfigurationsschritte** zum Installieren der Anwendungsdateien auf dem Hostsystem mit IBM Installation Manager und zum Konfigurieren von IBM SPSS Collaboration and Deployment Services Repository für die Ausführung mit dem angegebenen Cluster von Anwendungsservern und der angegebenen Repository-Datenbank.
- **Schritte nach der Installation** zum Starten von IBM SPSS Collaboration and Deployment Services Repository und zum Prüfen der Konnektivität.

Vor der Installation

Prüfen Sie vor der Installation von IBM SPSS Collaboration and Deployment Services mit einem WebSphere-Cluster-Server, ob Ihre Umgebung alle Hardware- und Softwareanforderungen auf allen Knoten des Clusters erfüllt. Berichte zur IBM Softwareproduktkompatibilität finden Sie im folgenden Dokument: https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html.

Wenn Sie den Server für IBM SPSS Collaboration and Deployment Services Repository in einer Umgebung mit Clusteranwendungsservern bereitstellen, muss jeder Anwendungsserver im Cluster für die gehosteten Anwendungskomponenten identisch konfiguriert sein und der Zugriff auf das Repository muss über eine hardware- oder softwarebasierte Lastausgleichsfunktion erfolgen. Diese Architektur ermöglicht die Verteilung der Verarbeitung auf mehrere Anwendungsserver und bietet Redundanzen für einen etwaigen Ausfall eines Servers.

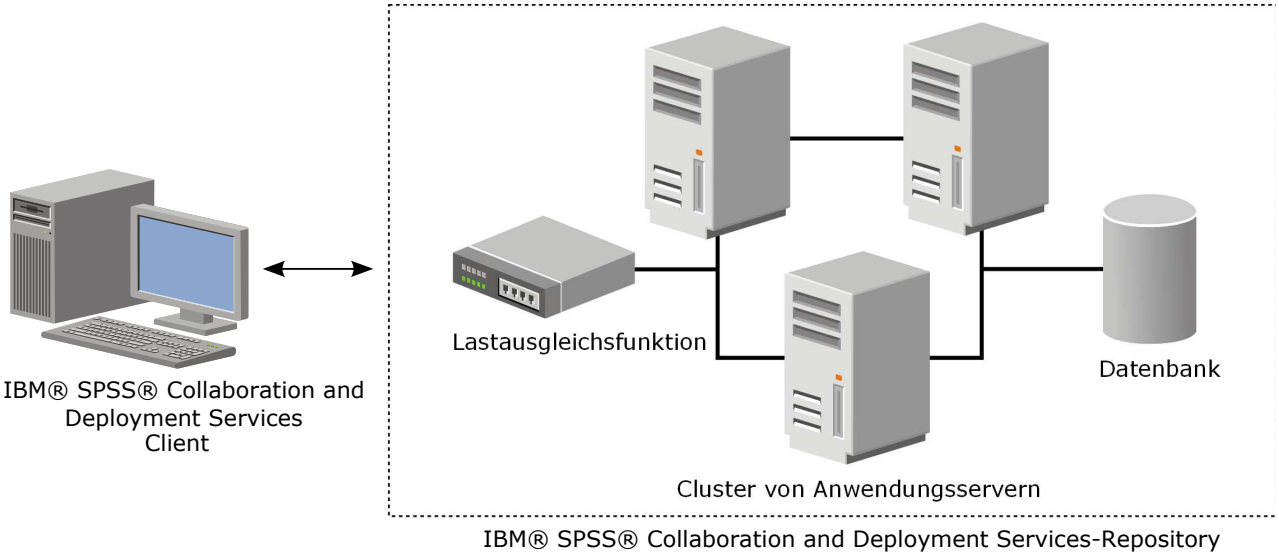

Abbildung 5. Clusterarchitektur

Der Prozess der Installation des Repository-Servers in einem Cluster beinhaltet folgende Schritte:

- Erstinstallation und -konfiguration von Anwendungskomponenten im Managementknoten des Clusters
- Anschließende Konfiguration von Clusterknoten

Installationsvoraussetzungen

- Die Hostsystemanforderungen müssen für alle Knoten des Clusters erfüllt sein.
- Alle Mitglieder des Clusters müssen auf demselben Betriebssystem ausgeführt werden wie der Hauptknoten (Managementknoten).
- Die IBM SPSS Collaboration and Deployment Services Repository-Datenbank muss bereits vorhanden sein und der Zugriff darauf muss vor der Installation des Repositorys möglich sein.
- Die Topologie des Anwendungsservers muss bereits vor der Installation des Repositorys vorhanden sein. Prüfen Sie, ob Zugriff auf den Cluster besteht und ob der Cluster an der Adresse der Lastausgleichsfunktion ordnungsgemäß ausgeführt wird.
- Das Repository-Installationsverzeichnis muss für alle Knoten im Cluster freigegeben sein.

WebSphere-Cluster-Server-Installation

Vor der Installation von IBM WebSphere muss IBM Installation Manager 1.8.9 oder höher bereits installiert sein. Weitere Informationen zur IBM Installation Manager-Installation finden Sie in https://jazz.net/wiki/bin/view/Deployment/InstallingUpdatingScriptingWithInstallationManager.

Je nach Ihrem Betriebssystem kann WebSphere über die Installation Manager-Schnittstelle, die Befehlszeile, eine Antwortdatei oder den Konsolenmodus installiert werden. Weitere Informationen finden Sie in https://www.ibm.com/support/knowledgecenter/SSEQTP_9.0.0/com.ibm.websphere.installation.base.doc/ae/tins_install.html.

Installieren von WebSphere mit IBM Installation Manager

1. Starten Sie Installation Manager.
   - GUI-Modus: `<IBM Installation Manager-Installationsverzeichnis>/eclipse/IBMIM`
   - Befehlszeilenmodus: `<IBM Installation Manager-Installationsverzeichnis>/eclipse/tools/imcl -c`
2. Konfigurieren Sie Installation Manager für die Verwendung eines Repositorys, das die Installationsdateien des IBM WebSphere-Anwendungsservers enthält.

3. Klicken Sie auf **Installieren**.
4. Wählen Sie die folgenden zu installierenden Produktangebote aus und klicken Sie auf **Weiter**.
   - IBM WebSphere Application Server Network Deployment
   - IBM SDK, Java Technology Edition, Version 8
5. Akzeptieren Sie die Bedingungen in den Lizenzvereinbarungen und klicken Sie auf **Weiter**.
6. Wählen Sie ein Verzeichnis für gemeinsam genutzte Ressourcen aus, das Ressourcen enthält, die von mehreren Installationspaketen gemeinsam genutzt werden können, und klicken Sie auf **Weiter**.
7. Wählen Sie alle gewünschte Sprachen aus, um übersetzten Inhalt zu installieren, und klicken Sie auf **Weiter**.
8. Wählen Sie die zu installierenden Funktionen aus und klicken Sie auf **Weiter**.
9. Prüfen Sie die Übersichtsinformationen und klicken Sie auf **Installieren**.

Wichtig: Der WebSphere-Anwendungsserver muss auf allen Knoten in der angegebenen WebSphere-Clustertopologie installiert werden. Wiederholen Sie die vorherigen Schritte auf allen Knoten im Cluster.

Cluster-Server-Einrichtung

Bestätigen Sie vor der Einrichtung eines Cluster-Servers, dass das mit IBM SPSS Collaboration and Deployment Services verwendete WebSphere-Profil für die Ausführung mit Java 7 SDK oder höher konfiguriert ist. Das folgende Beispiel veranschaulicht die Befehlsfolge für das Auflisten verfügbarer SDKs und Festlegen von Standard-SDKs.

```
<WebSphere-Installationsverzeichnis> \bin>managesdk.bat –listAvailable
CWSDK1003I: Verfügbare SDKs:
CWSDK1005I: SDK-Name: 8.0_64
CWSDK1001I: Die angeforderte managesdk-Task wurde erfolgreich ausgeführt.
<WebSphere-Installationsverzeichnis>\bin>managesdk.bat -setNewProfileDefault -sdkName 8.0_64
CWSDK1022I: Für die Erstellung neuer Profile wird jetzt der SDK-Name 8.0_64 verwendet.
CWSDK1001I: Die angeforderte managesdk-Task wurde erfolgreich ausgeführt.
```

Wichtig: Stellen Sie sicher, dass die Version von Java SDK auf allen Knoten im Cluster 7 oder höher ist.

Im Allgemeinen enthält eine Clustertopologie einen Managementknoten und ein paar verwaltete Knoten. WebSphere stellt ein Profilverwaltungsdienstprogramm bereit, mit dem Profile erstellt werden können. Beispiel:

1. Erstellen Sie das *Bereitstellungsverwaltungsprofil* auf dem *Management-Computer*:
   - Melden Sie sich am *Managementknoten* an und führen Sie das Profilverwaltungsdienstprogramm aus. Beispiel:
     – Windows:

       ```
       <WebSphere-Installationsverzeichnis>\bin> manageprofiles.bat –create –templatePath <WebSphere-Installationspfad>\profileTemplates\management –profileName XXXX -enableAdminSecurity true -adminUserName XXXX -adminPassword XXXX
       ```

     – Linux/UNIX:

       ```
       <WebSphere-Installationsverzeichnis>\bin> manageprofiles.sh –create –templatePath <WebSphere-Installationspfad>\profileTemplates\management –profileName XXXX -enableAdminSecurity true -adminUserName XXXX -adminPassword XXXX
       ```

2. Erstellen Sie das *Bereitstellungsverwaltungsprofil* auf dem *verwalteten Computer*:
   - Melden Sie sich am *verwalteten Knoten* an und führen Sie das Profilverwaltungsdienstprogramm aus. Beispiel:
     – Windows:

       ```
       <WebSphere-Installationsverzeichnis>\bin>manageprofiles.bat -create -templatePath <WebSphere-Installationsverzeichnis>\profileTemplates\managed -profileName XXXX
       ```

     – Linux/UNIX:

```
<WebSphere-Installationsverzeichnis>\bin>manageprofiles.sh -create -templatePath <WebSphere-
Installationsverzeichnis>\profileTemplates\managed -profileName XXXX
```

Wichtig: Wenn Ihre Clustertopologie mindestens zwei verwaltete Knoten aufweist, führen Sie diesen Befehl mehrmals aus, um verwaltete Knoten auf jedem verwalteten Computer zu erstellen.

Wenn alle Profile bereit sind, müssen Sie die Beziehung zwischen dem *Managementprofil* und den *verwalteten Profilen* erstellen. Wenn sich ein verwaltetes Profil auf einem anderen Computer als einem Managementprofil befindet, stellen Sie ordnungsgemäße Netzkonnektivität zwischen dem Management-Computer und dem verwalteten Computer sicher.

1. Starten Sie das *Managementprofil* auf dem *Managementknoten*:
   - Melden Sie sich am *Management-Computer* an und führen Sie den folgenden Befehl aus:
     - Windows:

       ```
       <WebSphere-Installationsverzeichnis>\profiles\<PROFILNAME>\bin>startManager.bat
       ```
     - Linux/UNIX:

       ```
       <WebSphere-Installationsverzeichnis>\profiles\<PROFILNAME>\bin>startManager.sh
       ```
2. Fügen Sie dem *Managementprofil verwaltete Knoten* hinzu:
   - Melden Sie sich am *verwalteten Computer* an und führen Sie den folgenden Befehl aus:
     - Windows:

       ```
       <WebSphere-Installationsverzeichnis>\profiles\<PROFILNAME>\bin>addNode.bat <Management-Host>
       ```
     - Linux/UNIX:

       ```
       <WebSphere-Installationsverzeichnis>\profiles\<PROFILNAME>\bin>addNode.sh <Management-Host> Port
       ```

       Dabei ist `<Management-Host>` der Hostname des Management-Computers. `Port` ist der Management-SOAP-Connector-Port des Managementprofils, das in der Datei `AboutThisProfile.txt` gespeichert ist. Wenn Ihre Clustertopologie mindestens zwei verwaltete Knoten aufweist, führen Sie diesen Befehl mehrmals für jedes verwaltete Profil aus.
3. Melden Sie sich an der WebSphere-Administrationskonsole an und erstellen Sie eine Clusterdefinition basierend auf den verwalteten Knoten:
   - Melden Sie sich an der WebSphere-Administrationskonsole des Managementprofils an: `https://Hostname:Port/ibm/console/logon.jsp`. Hierbei ist `Hostname` der Hostname des Management-Computers und `Port` ist die Portnummer der Administrationskonsole.
   - Gehen Sie zu **Server** > **Cluster** > **WebSphere Application Server-Cluster** und klicken Sie auf **Neu**, um eine Clusterdefinition zu erstellen.
   - Geben Sie einen Clusternamen an und klicken Sie auf **Weiter**.
   - Geben Sie einen Mitgliedsnamen für das erste Clustermitglied an und wählen Sie einen der verfügbaren Knoten aus. Klicken Sie auf **Weiter**.
   - Erstellen Sie weitere Clustermitglieder, indem Sie andere verfügbare Knoten hinzufügen.

Datenbank

Die Datenbank und IBM SPSS Collaboration and Deployment Services Repository müssen nicht auf demselben Server installiert werden, eine gewisse Konfiguration ist jedoch erforderlich, um Konnektivität sicherzustellen. Während der Installation werden Sie aufgefordert, den Datenbankservernamen, die Portnummer, den Benutzernamen und das Kennwort sowie den Namen der Datenbank anzugeben, die zum Speichern und Abrufen von Informationen verwendet werden soll.

Wichtig: Sie müssen die Datenbank vor der Installation manuell erstellen. Ein beliebiger gültiger Datenbankname kann verwendet werden, aber wenn keine zuvor erstellte Datenbank vorhanden ist, wird die Installation nicht fortgesetzt.

Es folgt ein SQL-Beispielscript für das Erstellen einer Db2-Datenbank namens `SPSSCDS`:

```
CREATE DATABASE SPSSCDS ON c:\ USING CODESET UTF-8 TERRITORY US COLLATE USING SYSTEM;
CONNECT TO SPSSCDS;
CREATE Bufferpool SPSS8K IMMEDIATE SIZE 250 AUTOMATIC PAGESIZE 8 K ;
CREATE REGULAR TABLESPACE SPSS8K PAGESIZE 8 K MANAGED BY AUTOMATIC STORAGE EXTENTSIZE 8 OVERHEAD 10.5 PREFETCHSIZE 8 TRANSFERRATE 0.14 BUFFERPOOL SPSS8K DROPPED TABLE RECOVERY ON;
COMMENT ON TABLESPACE SPSS8K IS '';
CREATE Bufferpool SPSSTEMP IMMEDIATE SIZE 250 PAGESIZE 32 K ;
CREATE SYSTEM TEMPORARY TABLESPACE SPSSTEMP PAGESIZE 32 K MANAGED BY AUTOMATIC STORAGE EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE 0.14 BUFFERPOOL "SPSSTEMP";
COMMENT ON TABLESPACE SPSSTEMP IS '';
CONNECT RESET;
CONNECT TO SPSSCDS;
GRANT DBADM,CREATETAB,BINDADD,CONNECT,CREATE_NOT_FENCED_ROUTINE,IMPLICIT_SCHEMA,LOAD,CREATE_EXTERNAL_ROUTINE,QUIESCE_CONNECT,SECADM ON DATABASE  TO USER CADSDBUSER;
CONNECT RESET;
UPDATE DB CFG FOR SPSSCDS USING LOGSECOND 200;
RESTART DATABASE SPSSCDS;
```

Installation

Wenn Sie den Server für IBM SPSS Collaboration and Deployment Services Repository auf einem WebSphere-Cluster-Server bereitstellen, müssen Sie sicherstellen, dass der Repository-Server auf dem gleichen Computer wie das WebSphere-Managementprofil installiert ist.

1. Melden Sie sich als Benutzer mit den entsprechenden Berechtigungen am Betriebssystem an.
2. Öffnen Sie IBM Installation Manager mit einer der folgenden Methoden:
   - GUI-Modus: `<IBM Installation Manager-Installationsverzeichnis>/eclipse/IBMIM`
   - Befehlszeilenmodus: `<IBM Installation Manager-Installationsverzeichnis>/eclipse/tools/imcl -c`
3. Wenn das Installationsrepository nicht konfiguriert ist, geben Sie den Repository-Pfad an (beispielsweise als Position im Hostdateisystem bzw. Netz oder als HTTP-Adresse).

   Anmerkung: Damit Sie erfolgreich auf ein Installationsrepository zugreifen können, darf der Pfad der Repository-Position kein Et-Zeichen (&) enthalten.
4. Wählen Sie im Hauptmenü die Option **Installieren** aus.
5. Wählen Sie "IBM SPSS Collaboration and Deployment Services" als zu installierendes Paket aus. Beispiel:
   - IBM SPSS Collaboration and Deployment Services - Repository Services
   - IBM SPSS Collaboration and Deployment Services Scoring Adapter for PMML
   - IBM SPSS Modeler Adapter for Collaboration and Deployment Services
6. Lesen Sie die Lizenzvereinbarung und akzeptieren Sie deren Bedingungen.
7. Geben Sie die Paketgruppe und das Installationsverzeichnis an:
   - Für die Installation von IBM SPSS Collaboration and Deployment Services Repository ist eine neue Paketgruppe erforderlich.
   - Geben Sie das Installationsverzeichnis für freigegebene Ressourcen an. Sie können das Verzeichnis für gemeinsam genutzte Ressourcen nur bei der ersten Installation eines Pakets angeben.
8. Prüfen Sie die zusammengefassten Informationen und fahren Sie mit der Installation fort. Die Anwendungsdateien werden im angegebenen Verzeichnis installiert, nachdem Sie auf **Installieren** geklickt haben.
9. Konfigurieren Sie das gemeinsam zu nutzende Installationsverzeichnis so, dass alle Mitglieder des Clusters darauf zugreifen können (indem Sie z. B. Dateifreigabe unter Windows oder NFS unter Linux/UNIX verwenden).

   Bei Problemen während der Installation können Sie diese mit den Protokollen von IBM Installation Manager beheben. Sie können über das Hauptmenü in IBM Installation Manager auf die Protokolldateien zugreifen.

Konfiguration

Nach der Ausführung der vorherigen Installationsschritte muss nun Folgendes vorliegen:

- Alle Mitglieder im WebSphere-Cluster werden auf demselben Betriebssystem ausgeführt wie der Hauptknoten (Managementknoten).

- Die Repository-Datenbank ist Repository-Datenbank und zugänglich.
- Das Installationsverzeichnis von IBM SPSS Collaboration and Deployment Services Repository wird von allen Knoten in Ihrem WebSphere-Cluster gemeinsam genutzt.

Bereitstellen des Repository-Servers auf Ihrem Cluster

1. Starten Sie das Konfigurationsdienstprogramm mit einer der folgenden Methoden:
   - GUI-Modus:
     - Windows: `<Repository-Installationsverzeichnis>\bin\configTool.bat`
     - Linux/UNIX: `<Repository-Installationsverzeichnis>/bin/configTool.sh`
   - Befehlszeilenmodus:
     - Windows: `<Repository-Installationsverzeichnis>\bin\cliConfigTool.bat`
     - Linux/UNIX: `<Repository-Installationsverzeichnis>/bin/cliConfigTool.sh`
2. Geben Sie den Typ des Anwendungsservers an. Wählen Sie bei einem WebSphere-Cluster **IBM WebSphere** aus.
3. Geben Sie die Einstellungen für den Anwendungsservertyp wie folgt an:
   - **WebSphere-Profilverzeichnis.** Die Verzeichnisposition des WebSphere-Serverprofils. Bei einem WebSphere-Cluster handelt es sich um den Pfad des Managementprofils. Andere WebSphere-Einstellungen wie das Stammverzeichnis der WebSphere-Installation, die Profiltopologie und der Knoten werden basierend auf den Profilinformationen automatisch eingetragen. Wenn Werte nicht automatisch eingetragen werden können, müssen Sie diese manuell angeben.
   - **URL-Präfix.** Die für den Zugriff auf den Repository-Server verwendete URL (z. B. `http://<Computer>:<Port>`). In einer Clusterumgebung ist der Port gewöhnlich die Portnummer der Lastausgleichsfunktion.
4. Geben Sie die Datenbankverbindungsinformationen wie folgt an:
   - **Datenbanktyp.** IBM Db2, SQL Server oder Oracle.
   - **Host.** Der Hostname bzw. die IP-Adresse des Datenbankservers.
   - **Port.** Der Zugriffsport für den Datenbankserver.
   - **Datenbankname.** Der Name der für das Repository zu verwendenden Datenbank.
   - **SID/Servicename.** Bei Oracle SID oder der Sicherheitskennung.
   - **Als Dienst ausführen.** Für Oracle, gibt an, dass die Verbindung zu einem Datenbankservice hergestellt wurde, anstatt über SID.
   - **Benutzername.** Der Name des Datenbankbenutzers.
   - **Kennwort.** Das Kennwort des Datenbankbenutzers.
5. Geben Sie bei der erneuten Verwendung einer Datenbank aus einer vorherigen Installation an, ob vorhandene Daten beibehalten oder verworfen werden sollen.
6. Geben Sie Optionen für den Keystore für Verschlüsselungsschlüssel an. Der Keystore ist eine verschlüsselte Datei, die den Schlüssel für die Entschlüsselung der vom Repository verwendeten Kennwörter enthält, beispielsweise das Repository-Administrationskennwort, das Kennwort für den Zugriff auf die Datenbank usw.
   - Geben Sie zur Wiederverwendung eines Keystores aus einer vorherigen Repository-Installation den Pfad und das Kennwort des Keystores an. Der Schlüssel aus dem alten Keystore wird extrahiert und im neuen Keystore verwendet. Beachten Sie, dass die JRE, die zum Ausführen des Anwendungsservers verwendet wird, mit der JRE kompatibel sein muss, die zum Erstellen der Verschlüsselungsschlüssel verwendet wurde.
   - Wenn Sie keinen bestehenden Keystore wiederverwenden, müssen Sie das Kennwort für den neuen Keystore angeben und bestätigen. Der Keystore wird unter `<Repository-Installationsverzeichnis>/keystore` erstellt.

Wichtig: Wenn Sie die Keystore-Datei verlieren, können mit der Anwendung keine Kennwörter mehr entschlüsselt werden, sodass diese nicht mehr verwendet werden kann. Sie muss erneut installiert werden. Ihnen wird empfohlen, Sicherungskopien der Keystore-Datei zu speichern.

7. Geben Sie den Kennwortwert an, der für die Erstellung des Administratorbenutzerkontos für das integrierte Repository (`admin`) verwendet werden soll. Dieses Kennwort wird bei der erstmaligen Anmeldung am Repository verwendet.
8. Wählen Sie den Bereitstellungsmodus aus ("Automatisch" oder "Manuell"). In diesem Beispiel wählen Sie **Automatisch** aus.
9. Prüfen Sie die zusammengefassten Informationen und fahren Sie mit der Konfiguration fort.

Konfigurieren des Clusters

Wenn der Server für IBM SPSS Collaboration and Deployment Services Repository auf Ihrem WebSphere-Cluster erfolgreich bereitgestellt wurde, sind einige externe Konfigurationsschritte erforderlich, damit Sie sicher sein können, dass der Server für jeden Knoten im Cluster oder über die Lastausgleichsfunktion zugänglich ist.

1. Legen Sie `CDS_HOME` für jeden Knoten fest:
   - Melden Sie sich an der WebSphere-Administrationskonsole an.
   - Gehen Sie zu **Umgebung** > **WebSphere-Variablen**
   - Prüfen Sie den Wert der Variablen **CDS_HOME** für jeden Knoten. Wenn sich ein WebSphere-Knoten auf einem anderen Server als dem Repository-Server befindet, aktualisieren Sie den Wert von CDS_HOME, sodass er auf das gemeinsam genutzte Installationsverzeichnis verweist (z. B. `\\<Management-Host>\SPSS\Deployment\8.2\Server`. Dabei ist `<Management-Host>` der Hostname des Computers, auf dem der Repository-Server installiert ist.
2. Legen Sie `Log4j Properties` für jeden Knoten fest:
   - Melden Sie sich an der WebSphere-Administrationskonsole an.
   - Suchen Sie die Eigenschaft `log4j.cnfiguration` unter **Server** > **WebSphere-Anwendungsserver** > **[Servername]** > **Java- und Prozessmanagement** > **Prozessdefinition** > **Java Virtual Machine** > **Benutzerdefinierte Eigenschaften**. Diese Eigenschaft gibt die Position an, an der das Protokollierungssystem auf die Konfigurationsdatei für die Protokollierung zugreifen kann. Normalerweise hat diese Eigenschaft den folgenden Wert: `file://${CDS_HOME}\platform\log4j.properties`. Wenn die Variable `CDS_HOME` unter Windows einen Laufwerkbuchstaben enthält, fügen Sie dem Wert `log4j.configuration` einen Schrägstrich (/) als Escapezeichen hinzu (z. B. `file:///${CDS_HOME}\platform\log4j.properties`).
   - Speichern und synchronisieren Sie Ihre Änderungen.

Lastausgleichsfunktion

Für den Zugriff auf das Repository in einer Clusterumgebung muss eine software- oder hardwarebasierte Lastausgleichsfunktion konfiguriert werden. WebSphere-Anwendungsserver enthalten integrierte Dienstprogramme mit einer softwarebasierten Lastausgleichsfunktion (zum Beispiel IBM HTTP Server). Die folgenden Schritte legen die Installation und Konfiguration von IBM HTTP Server dar.

Installieren von IBM HTTP Server

1. Starten Sie IBM Installation Manager.
2. Konfigurieren Sie Installation Manager für die Verwendung eines Repositorys, das die Installationsdateien von IBM HTTP Server enthält.
3. Klicken Sie auf **Installieren**.
4. Wählen Sie die folgenden zu installierenden Produktangebote aus und klicken Sie auf **Weiter**.
   - IBM HTTP Server for WebSphere Application Server
   - Web Server Plug-ins for IBM WebSphere Application Server

5. Akzeptieren Sie die Bedingungen in den Lizenzvereinbarungen und klicken Sie auf **Weiter**.
6. Geben Sie das Installationsverzeichnis an und klicken Sie auf **Weiter**.
7. Wählen Sie die zu installierenden Funktionen aus und klicken Sie auf **Weiter**.
8. Konfigurieren Sie die Details für IBM HTTP Server.
9. Prüfen Sie die Übersichtsinformationen und klicken Sie auf **Installieren**.

Erstellen einer Web-Server-Definition in Ihrem WebSphere-Cluster

1. Melden Sie sich an der WebSphere-Administrationskonsole für das Managementprofil an: `https://Hostname:Port/ibm/console/logon.jsp`. Hierbei ist `Hostname` der Hostname des Management-Computers und `Port` ist der Port der Administrationskonsole.
2. Gehen Sie zu **Servertypen** > **Web-Server** und klicken Sie auf **Neu**, um eine neue Web-Server-Definition zu erstellen.
3. Geben Sie den Servernamen an und wählen Sie den Knoten aus, der dem Web-Server entspricht, den Sie hinzufügen wollen. In der Regel muss sich der Knoten auf dem Server befinden, auf dem der HTTP-Server installiert ist. Wählen Sie **IBM HTTP Server** als Typ aus und klicken Sie auf **Weiter**.
4. Wählen Sie die Vorlage aus, die dem Server entspricht, den Sie erstellen wollen, und klicken Sie auf **Weiter**. In diesem Beispiel wird der Standardwert verwendet.
5. Geben Sie Eigenschaften für den neuen Web-Server an.
6. Prüfen Sie die Zusammenfassung der neuen Web-Server-Definition und klicken Sie auf **Fertigstellen**.
7. Speichern Sie Ihre Änderungen.

Konfigurieren des Web-Servers

1. Melden Sie sich an der WebSphere-Administrationskonsole für das Managementprofil an.
2. Suchen Sie die Datei `conf.httpd` unter **Server** > **Servertypen** > **Web-Server** > **[Servername]**. Fügen Sie der Datei das folgende Script hinzu:

   ```
   LoadModule was_ap22_module "<Plug-in-Verzeichnis>\bin\32bits\mod_was_ap22_http.dll"
   WebSpherePluginConfig "<Plug-in-Verzeichnis>\config\<Web-Server-Name>\plugin-cfg.xml"
   ```

   Dabei ist `<Plug-in-Verzeichnis>` das Plug-in-Installationsverzeichnis des Web-Servers und `<Web-Server-Name>` ist der Name Ihres Web-Servers.
3. Gehen Sie zu **Server** > **Servertypen** > **Web-Server**, wählen Sie Ihren Web-Server aus und klicken Sie auf **Plug-in generieren**.
4. Klicken Sie auf **Plug-in weitergeben**, um das Plug-in rundzusenden.
5. Gehen Sie zu **Server** > **Servertypen** > **Web-Server** > **[Servername]** und zeigen Sie `plugin-cfg.xml` an, um zu bestätigen, dass alle URIs für IBM SPSS Collaboration and Deployment Services generiert wurden (z. B. `<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/admin/*"/>`.

Festlegen der Eigenschaft für das URL-Präfix

In einer Clusterumgebung wird die Repository-Konfigurationseigenschaft **URL_Prefix** für das Routing von vom Server eingeleiteten HTTP-Anforderungen verwendet. Die Eigenschaft muss auf die URL der Lastausgleichsfunktion gesetzt werden. Beachten Sie, dass Sie diese Eigenschaft bei der ursprünglichen Ausführung des Konfigurationsdienstprogramms von IBM SPSS Collaboration and Deployment Services Repository festlegen können.

So aktualisieren oder legen Sie den Wert der Eigenschaft für das URL-Präfix nach der Repository-Konfiguration fest:

1. Starten Sie ein einzelnes Clustermitglied.
2. Öffnen Sie die browserbasierte Instanz von IBM SPSS Deployment Manager, indem Sie zu `http://<Repository-Host>:<Portnummer>/security/login` navigieren und sich mit dem Administratorkonto anmelden, das während der Repository-Konfiguration erstellt wurde.

3. Aktualisieren Sie die Konfigurationseigenschaft **URL_Prefix** mit der URL der Lastausgleichsfunktion für den Cluster. Speichern Sie Ihre Änderungen.
4. Stoppen Sie das gerade ausgeführte Clustermitglied. Starten Sie den Cluster.

Nach der Installation

Die folgende Checkliste soll Ihnen als Leitfaden für die Schritte nach der Installation dienen:

1. Starten Sie den Server und prüfen Sie die Konnektivität (Anweisungen hierzu im folgenden Abschnitt).
2. Installieren Sie alle Inhaltsadapter, die Sie für die Verwendung von IBM SPSS Collaboration and Deployment Services Repository mit anderen SPSS-Produkten wie IBM SPSS Modeler oder IBM SPSS Statistics benötigen.
3. Installieren Sie bei Bedarf IBM SPSS Collaboration and Deployment Services Remote Process Server und IBM SPSS Collaboration and Deployment Services - Essentials for Python. Weitere Informationen finden Sie in den Installationsanweisungen für diese Komponenten.
4. Installieren Sie Clients für IBM SPSS Collaboration and Deployment Services, einschließlichIBM SPSS Deployment Manager. Weitere Informationen finden Sie in den Installationsanweisungen der Clientanwendung.
5. Erstellen Sie mit IBM SPSS Deployment Manager Repository-Benutzer und -Gruppen und weisen Sie ihnen über Rollen Anwendungsberechtigungen zu. Weitere Informationen finden Sie im Administratorhandbuch zu IBM SPSS Collaboration and Deployment Services.

Wenn während dieser Schritte nach der Installation Probleme auftreten, konsultieren Sie das Handbuch zur Fehlerbehebung zu IBM SPSS Collaboration and Deployment Services.

Starten des Repository-Servers

Bei WebSphere-Cluster-Servern wird der Repository-Server automatisch gestartet, wenn Sie den Anwendungsserver starten. Starten Sie den Anwendungsserver mithilfe der Scripts, die mit den WebSphere-Verwaltungstools bereitgestellt werden.

1. Melden Sie sich am Management-Computer an und starten Sie den Managementknoten:
   - Windows: `<WebSphere-Installationsverzeichnis>\profiles\<PROFILNAME>\bin>startManager.bat`
   - Linux/UNIX: `<WebSphere-Installationsverzeichnis>\profiles\<PROFILNAME>\bin>startManager.sh`
2. Melden Sie sich auf jedem Computer an und starten Sie jeden Agenten für verwaltete Knoten:
   - Windows: `<WebSphere-Installationsverzeichnis>\profiles\<PROFILNAME>\bin>startNode.bat`
   - Linux/UNIX: `<WebSphere-Installationsverzeichnis>\profiles\<PROFILNAME>\bin>startNode.sh`
3. Melden Sie sich an der WebSphere-Administrationskonsole für den Managementknoten (`http://Hostname:Port/ibm/console`) an. Gehen Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**, wählen Sie jeden Knoten aus und klicken Sie auf **Starten**.
4. Gehen Sie zu **Server** > **Servertypen** > **Web-Server** und klicken Sie auf **Starten**.

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 Administratorberechtigungen (Windows).

Prüfen der Konnektivität

Sie können prüfen, ob der Server für IBM SPSS Collaboration and Deployment Services Repository ausgeführt wird, indem Sie auf die browserbasierte Instanz von IBM SPSS Deployment Manager in einem unterstützten Web-Browser unter `http://<Repository-Host>:<Portnummer>/security/login` zugreifen. Wenn das Tool nicht gestartet wird, wird der Server wahrscheinlich nicht ausgeführt. Weitere Informationen zu

unterstützten Web-Browsern finden Sie in den Berichten zur IBM Softwareproduktkompatibilität unter https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html.

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

Diese Informationen können technische Ungenauigkeiten oder typografische Fehler enthalten. 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

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 Corporation 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 von Microsoft Corporation in den USA und/oder anderen Ländern.

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

Java und alle 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

Numerische Stichwörter

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

Gedruckt in Deutschland