IBM SPSS Collaboration and Deployment Services Repository 8.3

Installations- und Konfigurationshandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen” auf Seite 79 gelesen werden.

Produktinformation

Diese Ausgabe bezieht sich auf Version 8, Release 3, 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 der Vorhersageanalyse gestattet.

IBM SPSS Collaboration and Deployment Services bietet eine zentrale, sichere und überprüfbare Speicherung von Analyseeinrichtungen und erweiterte Funktionen für Verwaltung und Steuerung von Analyseprozessen zur Vorhersage sowie ausgereifte Mechanismen zur Bereitstellung der Ergebnisse der analytischen Verarbeitung für die Benutzer. 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

Mit IBM SPSS Collaboration and Deployment Services können Sie verschiedene analytische Informationen sicher verwalten und eine bessere Zusammenarbeit zwischen den Personen fördern, die diese erstellen, und jenen, die sie nutzen. Darüber hinaus stellen die Bereitstellungsfunktionen sicher, dass die erforderlichen Informationen zu den Personen gelangen, damit diese rechtzeitig entsprechende Maßnahmen ergreifen können.

Zusammenarbeit

Mit dem Begriff *Zusammenarbeit* (Collaboration) wird die Möglichkeit bezeichnet, 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. Dieser Ort muss eine Versionssteuerung für die Dateien aufweisen, damit die Entwicklung der Analyse verwaltet werden kann. Sicherheit ist erforderlich, um den Zugriff auf die Dateien und das Ändern dieser zu steuern. Und schließlich wird ein Sicherungs- und Wiederherstellungsmechanismus benötigt, damit das Unternehmen vor dem Verlust dieser wichtigen Informationen geschützt ist.

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. Mit Produkten wie IBM SPSS Statistics und IBM SPSS Modeler kann direkt auf die Dateien im Repository zugegriffen werden. 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. Versionssteuerung und Objektversionsbeschriftungen stellen sicher, das bei Produktionsprozessen die korrekten Versionen der Informationen verwendet werden. Zu guter Letzt bieten Protokollierfunktionen die Möglichkeit, Datei- und Systemmodifizierungen nachzuverfolgen.

Bereitstellung

Damit die Vorteile der Vorhersageanalyse voll ausgeschöpft werden können, müssen die analytischen Informationen bei Geschäftsentscheidungen verfügbar sein. Durch die Bereitstellung wird eine Brücke zwischen Analysen und Maßnahmen geschlagen, indem die Ergebnisse bei Personen oder Prozessen nach einem bestimmten Zeitplan oder in Echtzeit verfügbar sind.

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 bestimmte Empfänger gesendet werden. Auf im Repository gespeicherte Ergebnisse kann mit der IBM SPSS Collaboration and Deployment Services Deployment Portal-Schnittstelle von jedem Benutzer mit ausreichenden Berechtigungen zugegriffen werden. Die Jobs selbst können laut einem definierten Zeitplan oder als Reaktion auf Systemereignisse ausgeführt 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 Client-Anwendung verwendet werden, sodass die Erstellung benutzerdefinierter Schnittstellen zum Definieren des Prozesses möglich wird.

Die Bereitstellungsfunktionen von IBM SPSS Collaboration and Deployment Services wurden so entwickelt, dass sie sich problemlos in die Infrastruktur Ihres Unternehmens integrieren lassen. Durch Single Sign-On müssen Berechtigungsnachweise zu verschiedenen Phasen des Prozesses nicht manuell bereitgestellt werden. Außerdem kann das System so konfiguriert werden, dass es mit Publikation 140-2 des Federal Information Processing Standard kompatibel ist.

Systemarchitektur

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

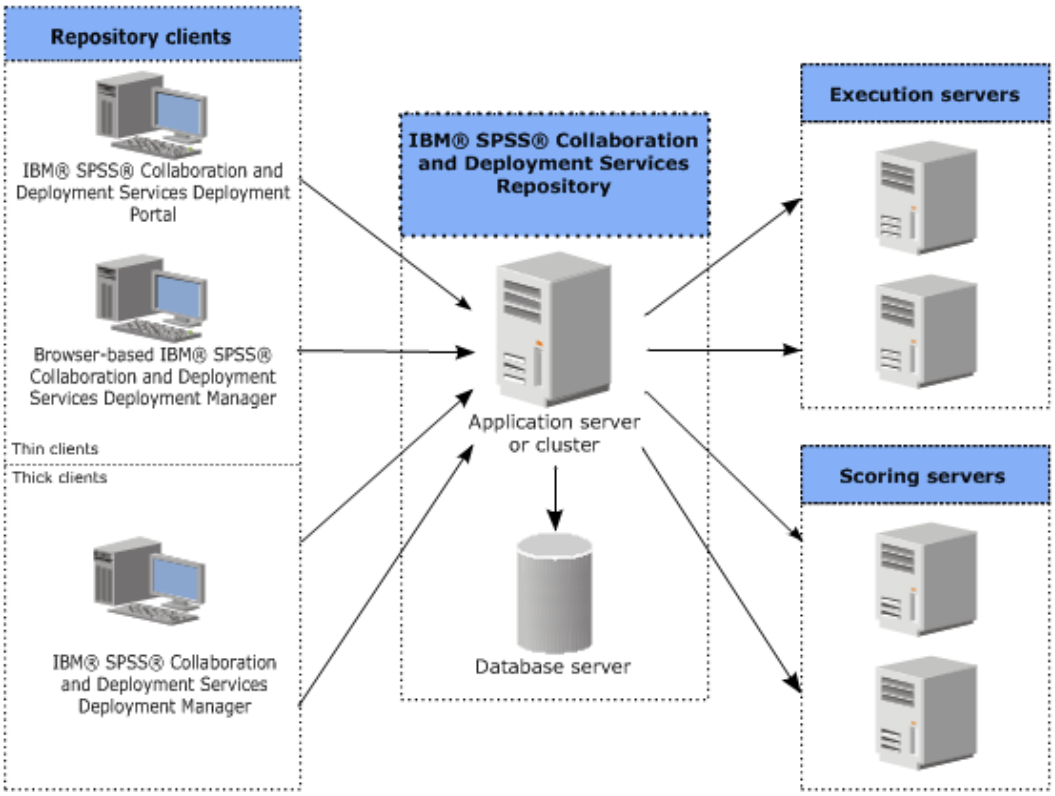

Abbildung 1. IBM SPSS Collaboration and Deployment Services - Architektur

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
- Browserbasierter 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
- Prüfungswesen

Konfigurationsoptionen für das Repository werden über den IBM SPSS Deployment Manager oder den browserbasierten 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, z. B. die Aktualisierung von Modellen oder das Generieren von Scores, zu planen, zu automatisieren und auszuführen.

Die Clientanwendung ermöglicht dem Benutzer die Ausführung folgender Aufgaben:

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

Außerdem ermöglicht die Clientanwendung den Benutzern, administrative Aufgaben für IBM SPSS Collaboration and Deployment Services auszuführen, z. B.:

- Verwalten von Benutzern
- Konfigurieren von Sicherheitsprovidern
- Zuweisen von Rollen und Aktionen

Browserbasierter IBM SPSS Deployment Manager

Der browserbasierte IBM SPSS Deployment Manager ist eine Thin-Client-Schnittstelle zum Durchführen von Setup- und Systemverwaltungsaufgaben wie den folgenden:

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

Benutzer, die keine Administratoren sind, können alle diese Aufgaben ebenfalls durchführen, sofern ihren Anmeldeberechtigungsnachweisen die entsprechenden Aktionen zugewiesen sind. Die Aktionen werden von einem Administrator zugewiesen.

In der Regel erfolgt der Zugriff auf den browserbasierten IBM SPSS Deployment Manager über folgende URL:

```
http://<Host-IP-Adresse>:<Port>/security/login
```

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

Wenn Ihre Umgebung so konfiguriert ist, dass für Serververbindungen ein benutzerdefinierter Kontextpfad verwendet wird, schließen Sie diesen Pfad in die URL ein.

```
http://<Host-IP-Adresse>:<port>/<Kontextpfad>/security/login
```

IBM SPSS Collaboration and Deployment Services Deployment Portal

IBM SPSS Collaboration and Deployment Services Deployment Portal ist eine Thin-Client-Schnittstelle für den Zugriff auf das Repository. Im Gegensatz zum browserbasierten IBM SPSS Deployment Manager, das 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 bietet die folgenden Funktionen:

- Durchsuchen des Repository-Inhalts nach Ordner
- Öffnen veröffentlichten Inhalts
- Ausführen von Jobs und Berichten
- Generieren von Scores anhand von im Repository gespeicherten Modellen
- Durchsuchen des Repository-Inhalts

- Anzeigen von Inhaltseigenschaften
- Zugreifen auf bestimmte Benutzervorgaben wie E-Mail-Adresse und Kennwort, allgemeine Optionen, Abonnements und Optionen für Ausgabedateiformate

In der Regel erfolgt der Zugriff auf die Homepage über folgende URL:

```
http://<Host-IP-Adresse>:<Port>/peb
```

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

Wenn Ihre Umgebung so konfiguriert ist, dass für Serververbindungen ein benutzerdefinierter Kontextpfad verwendet wird, schließen Sie diesen Pfad in die URL ein.

```
http://<Host-IP-Adresse>:<Port>/<Kontextpfad>/peb
```

Ausführungsserver

Ausführungsserver ermöglichen die Ausführung von Ressourcen, die im Repository gespeichert sind. Wenn eine Ressource in einem Job zur Ausführung enthalten ist, umfasst die Jobschrittdefinition die Angabe des Ausführungsservers, der zum Durchführen des Schritts verwendet wird. Der Ausführungsservertyp hängt von der Ressource ab.

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

- **Fernverarbeitung**. Ein Fernverarbeitungs-Ausführungsserver macht es möglich, dass Prozesse auf entfernten Servern initiiert und überwacht werden können. 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 maximal 16 gleichzeitige Jobs auf einem einzigen Fernverarbeitungsserver ausgeführt werden. Wird die Anzahl von 16 gleichzeitigen Jobs 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 über das Starten und Stoppen des Fernverarbeitungsservers im Handbuch zu IBM SPSS Collaboration and Deployment Services Remote Process Server.

Ausführungsserver, die andere spezifische Ressourcentypen verarbeiten, können zum System hinzugefügt werden, indem die entsprechenden Adapter installiert werden. Weitere Informationen finden Sie in der Dokumentation dieser Ressourcentypen.

Weisen Sie beim Erstellen von Jobs jedem Schritt in diesen Jobs 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.

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 die IBM SPSS Collaboration and Deployment Services-Protokolldateien aufgezeichnet werden (standardmäßig `<UserProfile>\AppData\Roaming\SPSSInc\Deployment Manager`).

Kapitel 2. Installation

In diesem Kapitel finden Sie Informationen zur Installation des IBM SPSS Collaboration and Deployment Services Repositorys. Der Prozess umfasst eine Reihe von Schritten zur Vorinstallation, Installation und Konfiguration sowie Schritte nach der Installation.

- Die Schritte zur **Vorinstallation** für die Einrichtung der Anwendungsumgebung umfassen die Ermittlung der Systemanforderungen basierend auf dem Installationstyp und der geplanten Systemverwendung, die Bereitstellung des Systems bzw. der Systeme, auf denen der Anwendungsserver oder Server-Cluster ausgeführt werden soll, die Sicherstellung, dass der bzw. die Server alle Hardware- und Softwareanforderungen erfüllt/erfüllen, die Konfiguration des Anwendungsservers oder Clusters sowie die Konfiguration der Datenbank. Es kann auch erforderlich sein, die Inhalte aus der vorherigen Installation mithilfe von Tools zum Kopieren von Datenbanken in die neue Datenbank zu migrieren.
- Die Schritte zur **Installation und Konfiguration** umfassen die Installation der Anwendungsdateien auf dem Hostsystem mit IBM Installation Manager und die nachfolgende Konfiguration des IBM SPSS Collaboration and Deployment Services Repositorys zur Ausführung des Repositorys mit dem festgelegten Anwendungsserver oder Server-Cluster und der Repository-Datenbank.
- Die Schritte **nach der Installation** umfassen das Starten des IBM SPSS Collaboration and Deployment Services Repositorys, das Prüfen der Konnektivität, das Konfigurieren des automatischen Starts sowie das Installieren zusätzlicher Datenbanktreiber, optionaler Komponenten und Inhaltsadapter für andere Produkte von IBM SPSS.

Beachten Sie, dass in einigen Umgebungen für die Bereitstellung des IBM SPSS Collaboration and Deployment Services Repositorys auch eine Reihe von optionalen unternehmensweiten Konfigurationsschritten ausgeführt werden müssen. Diese beziehen sich auf die Anwendungssicherheit, die Zugriffssteuerung und Benachrichtigungsfunktionen beziehen.

- E-Mail- und RSS-Benachrichtigungen. Weitere Informationen finden Sie im entsprechenden Kapitel im Administratorhandbuch.
- Sichere Repository-Verbindung. Weitere Informationen finden Sie im Thema Kapitel 8, „Verwenden von SSL zur sicheren Datenübertragung", auf Seite 61.
- FIPS 140-2-Sicherheit und sichere Verbindung mit der Repository-Datenbank. Weitere Informationen finden Sie im Thema Kapitel 7, „FIPS 140–2-Konformität", auf Seite 59.
- Single Sign-on. Weitere Informationen finden Sie im Thema Kapitel 5, „Single Sign-on", auf Seite 43.

Installationsvorbereitung

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

Die folgende Checkliste soll Ihnen als Leitfaden für den Prozess der Installationsvorbereitung dienen:

- Bestimmen Sie basierend auf der geplanten Systemverwendung und den entsprechenden Systemanforderungen den Installationstyp.
- Stellen Sie das System bzw. die Systeme bereit, um den Anwendungsserver oder den Server-Cluster auszuführen. Stellen Sie sicher, dass der/die Server alle Hardware- und Softwareanforderungen erfüllt.
- Prüfen Sie bei der Installation die Benutzerberechtigung und Hostdateisystemberechtigungen.
- Konfigurieren Sie den Anwendungsserver oder den Cluster.
- Konfigurieren Sie die Datenbank. Falls erforderlich, migrieren Sie die Inhalte aus der vorherigen Installation mithilfe von Tools zum Kopieren von Datenbankenin die neue Datenbank. Weitere Informationen finden Sie im Thema Kapitel 3, „Migration", auf Seite 37.

Planen Ihrer Installation

Vor der Installation von IBM SPSS Collaboration and Deployment Services Repository müssen Sie den Installationstyp bestimmen, damit Sie die Anwendungsumgebung einrichten können. IBM SPSS Collaboration and Deployment Services Repository ist ein auf Unternehmen abgestimmtes System, das die Integration in mehrere Komponenten von IBM Corp. sowie Komponenten und Technologien anderer Anbieter erfordert. In seiner einfachsten Konfiguration ist eine bereits vorhandene Installation eines Anwendungsservers erforderlich, damit die Web-Services ausgeführt werden können, über die die Funktionalität der Anwendung aktiviert wird, sowie eine relationale Datenbank (z. B. IBM Db2 UDB, Oracle oder Microsoft SQL Server), damit analytische Artefakte und Anwendungseinstellungen gespeichert werden können.

Verwenden Sie bei der Planung Ihrer Installation folgende Richtlinien:

- In Betriebsumgebungen muss das Repository auf einem System auf Serverniveau installiert werden. Weitere Informationen finden Sie im Thema „Hostsystemanforderungen” auf Seite 8. Durch das Ausführen der Repository-Datenbank auf einem separaten dedizierten Server kann die Gesamtleistung des Systems verbessert werden.
- In Unternehmensumgebungen mit großen Systembelastungen (z. B. Generierung von Echtzeitscores) und einer größere Anzahl an Benutzern wird eine Hochskalierung mit einem Cluster von Anwendungsservern anstelle eines eigenständigen Anwendungsservers empfohlen.
- Das Repository kann zwar zu Bildungs- oder Demonstrationszwecken auf einer Desktop-Workstation oder einem Notebook installiert und ausgeführt werden, allerdings kann es auf solchen Systemen nicht in einer Produktionsumgebung ausgeführt werden.

Bei der Planung der Bereitstellung Ihres IBM SPSS Collaboration and Deployment Services Repositorys müssen Sie auch die zusätzlichen Anforderungen einer Produktionsumgebung berücksichtigen. Damit analytische Artefakte und Scoring verarbeitet werden können, kann es beispielsweise erforderlich sein, Ausführungsserver einzurichten, wie z. B. IBM SPSS Statistics- und IBM SPSS Modeler-Server, für die zudem dedizierte Hardware- und Netzressourcen erforderlich sein können. Damit die E-Mail-Benachrichtigungsfunktion aktiviert werden kann, muss ein SMTP-Server verfügbar sein. Es kann auch 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 folgende Hardware- und Softwareanforderungen erfüllt sind. Wenn Sie die Installation mit einem Cluster von Anwendungsservern ausführen, müssen die Anforderungen auf 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 RAM-Anzahl ist für das erfolgreiche Installieren und Starten des Repositorys mindestens erforderlich. Abhängig von den Typen der analytischen Verarbeitung, die von IBM SPSS Collaboration and Deployment Services durchgeführt wird, können die Anforderungen an den Laufzeitspeicher erheblich höher sein und einen großen Teil des RAM verwenden, der in der Regel auf einem System auf Serverniveau installiert ist. Beachten Sie, dass für die Installation von Repository-Adaptern für andere Produkte von IBM SPSS, wie z. B. IBM SPSS Modeler-Adapter, zusätzlicher dedizierter Hauptspeicher erforderlich ist. Es wird empfohlen, bei der Schätzung des Speicherbedarfs für Ihren ausgewählten Anwendungsserver die Anwendungsserverdokumentation zu konsultieren.

Bei der Installation in WebSphere muss das mit IBM SPSS Collaboration and Deployment Services verwendete WebSphere-Profil für die Ausführung mit Java SDK 7 oder höher konfiguriert werden. Siehe „WebSphere” auf Seite 10.

Zusätzliche Anforderungen

IBM Installation Manager (für alle Betriebssysteme)

IBM Installation Manager 1.9.1 oder höher muss installiert und konfiguriert sein, damit ein Repository mit IBM SPSS Collaboration and Deployment Services-Installationsdateien verwendet werden kann.

Wenn IBM Installation Manager noch nicht auf dem System vorhanden ist, wird dieses Programm automatisch installiert, wenn Sie die Installation von IBM SPSS Collaboration and Deployment Services starten. Wenn Sie über eine ältere Version von IBM Installation Manager verfügen, müssen Sie diese im Rahmen der Installation aktualisieren.

Wenn IBM Installation Manager nicht automatisch installiert wird und auf dem System nicht vorhanden ist, können Sie IBM Installation Manager über die IBM Corp. Unterstützungssite (http://www.ibm.com/support) herunterladen und installieren. Informationen zur Speicherposition für den Download und zu Benutzerdaten finden Sie in der Dokumentation zu IBM Installation Manager: http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.

UNIX und Linux

- Die X Windows System Terminal-Software ist für die grafisch orientierte Installation des IBM SPSS Collaboration and Deployment Services Repositorys erforderlich. Alternativ kann ggf. der Server im automatischen Modus ausgeführt werden (Java-Befehlszeilenoption `-Djava.awt.headless=true`) oder das PJA-Toolkit (Pure Java AWT) verwendet werden.

Benutzer- und Dateisystemberechtigungen

Als allgemeine Regel gilt, dass Sie das Repository mit den gleichen Benutzerberechtigungen installieren und konfigurieren sollten, die auch für die Installation und Konfiguration des Anwendungsservers verwendet wurden. Weitere Informationen zur Unterstützung von Installationen durch Benutzer ohne Rootberechtigung/ohne Administratorrechte finden Sie in der Herstellerdokumentation zu Ihrem Anwendungsserver.

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

- Schreibberechtigungen für das Installationsverzeichnis und Unterverzeichnisse.
- Schreibberechtigungen für die Bereitstellungs- und Konfigurationsverzeichnisse sowie Lese- und Ausführungsberechtigungen für andere Anwendungsserververzeichnisse.
- Wenn das Repository mit einem Cluster von Anwendungsservern installiert wird, muss das Repository-Installationsverzeichnis auf dem System, auf dem das Managementprofil gehostet wird (herkömmliches WebSphere-Profil oder Liberty-Profil), freigegeben werden, damit es auf allen Knoten des Clusters verfügbar ist.

Anmerkung: Bei der Installation von IBM SPSS-Inhaltsadaptern müssen Sie denselben Benutzer verwenden, der auch bei der IBM SPSS Collaboration and Deployment Services Repository-Installation verwendet wurde.

Wichtig: Wenn Sie das IBM SPSS Collaboration and Deployment Services Repository unter Windows über ein Administratorkonto installieren, müssen Sie die Administratorrechte verwenden, um alle zugehörigen Dienstprogramme und Scripts ausführen zu können, z. B. das Konfigurationsdienstprogramm.

Virtualisierung

IBM SPSS Collaboration and Deployment Services Repository- oder Clientkomponenten können in virtualisierten Umgebungen bereitgestellt werden, die von Software anderer Anbieter bereitgestellt werden. Zur Vereinfachung der Bereitstellung einer Entwicklungs- oder Testumgebung kann ein Systemadministrator beispielsweise einen virtuellen Server konfigurieren, auf dem IBM SPSS Collaboration and Deployment Services installiert werden soll. Die IBM SPSS Collaboration and Deployment Services-Hostingkomponen-

ten der virtuellen Maschinen müssen die Systemmindestvoraussetzung erfüllen. Weitere Informationen finden Sie im Abschnitt „Hostsystemanforderungen” auf Seite 8.

Davon ausgehend, dass die konfigurierte virtualisierte Umgebung die Systemmindestvoraussetzung erfüllt, werden beim IBM SPSS Collaboration and Deployment Services Repository oder den Clientinstallationen keine Leistungseinbußen erwartet. Es sei jedoch darauf hingewiesen, dass virtualisierte Systeme verfügbare physische Ressourcen gemeinsam nutzen können und Ressourcenkonflikte auf Systemen mit einer hohen Verarbeitungslast zu Leistungseinbußen bei den gehosteten IBM SPSS Collaboration and Deployment Services-Installationen führen können.

Beachten Sie, dass es weitere Einschränkungen bei der Bereitstellung in virtualisierten Umgebungen geben kann, wenn der Anwendungsserver, der für die Ausführung des Repositorys verwendet wird, in diesen Umgebungen nicht bereitgestellt werden kann.

Anwendungsserver

Vor der Installation des IBM SPSS Collaboration and Deployment Services Repositorys muss ein unterstützter Anwendungsserver oder ein Server-Cluster installiert werden und zugänglich sein.

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

Wenn das Repository erneut installiert wird, erstellen Sie den Anwendungsserver erneut, indem Sie beispielsweise ein neues WebSphere-Profil bereitstellen. Stellen Sie sicher, dass die aktuellen Patches des entsprechenden Anbieters auf die Anwendungsserverinstallationen angewendet werden. Wenn Sie das IBM SPSS Collaboration and Deployment Services Repository mit einem Cluster von Anwendungsservern installieren, müssen alle Clusterknoten die gleiche Version des Anwendungsservers aufweisen und unter demselben Betriebssystem ausgeführt werden.

Der Anwendungsserver muss mit einer entsprechenden JRE eingerichtet werden. Stellen Sie sicher, dass Sie Java im 64-Bit-Modus ausführen und dass Ihr Anwendungsserver im 64-Bit-Modus einwandfrei arbeitet, bevor Sie versuchen, das IBM SPSS Collaboration and Deployment Services Repository zu installieren. Wenn Sie beispielsweise JBoss verwenden und sowohl das 32-Bit- als auch das 64-Bit-JDK installiert haben, sollten Sie die JVM für die Ausführung im 64-Bit-Modus konfigurieren, indem Sie die Option `-d64` für den Java-Befehl angeben. Für die Bereitstellung im WebSphere Liberty-Profil wird die IBM JRE mit IBM SPSS Collaboration and Deployment Services gebündelt. Weitere Informationen finden Sie in der Herstellerdokumentation zum Anwendungsserver.

Wichtig: Wenn Sie Verbindungen von Web-Browsern unterstützen möchten, deren Cookies inaktiviert sind, müssen Sie die URL-Umschreibung für Ihren Anwendungsserver aktivieren. In WebSphere ist diese Einstellung beispielsweise auf der Administrationskonsole unter **Anwendungsserver** > ***Server1*** > **Web-Container** > **Sitzungsmanagement** > **URL-Umschreibung aktivieren** verfügbar. Weitere Informationen finden Sie in der Dokumentation zum Anwendungsserver.

Einschränkung: Die URL-Umschreibung wird nicht von Funktionen unterstützt, die inzwischen veraltet sind. Bei diesen Funktionen müssen Cookies möglicherweise aktiviert werden.

WebSphere

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

Vor der Installation mit einem eigenständigen WebSphere-Server

- Erstellen Sie mit der Standardprofilvorlage der Anwendung für jede Installation ein neues Profil.

Vor der Installation mit einem verwalteten WebSphere-Server

- Erstellen Sie das Bereitstellungsmanagementprofil.
- Starten Sie das Managementprofil.
- Erstellen Sie das verwaltete Profil.
- Fügen Sie dem Managementprofil einen verwalteten Knoten hinzu.
- Erstellen Sie über die WebSphere-Konsole den verwalteten Server auf Basis des verwalteten Knotens.

Vor der Installation mit einem WebSphere-Cluster

- Erstellen Sie den Cluster und stellen Sie sicher, dass über die Lastausgleichsfunktion darauf zugegriffen werden kann.

Vor der Installation mit einer WebSphere Application Server Network Deployment-Topologie

Erhöhen Sie die standardmäßige Hauptspeicherkonfiguration für den WebSphere Deployment Manager-Prozess (**dmgr**) und die WebSphere Nodeagent-Prozesse. Welche Speicherbedarf tatsächlich erforderlich ist, hängt von Ihrem System ab. Bei einer Mindestspeicherkonfiguration würde der Speicher beispielsweise wie folgt erhöht:

- Erhöhen Sie beim WebSphere Deployment Manager-Prozess die Mindestgröße des Heapspeichers auf 512 und die maximale Größe des Heapspeichers auf 1024
- Erhöhen Sie bei den WebSphere Nodeagent-Prozessen die Mindestgröße des Heapspeichers auf 256 und die maximale Größe des Heapspeichers auf 512

Anmerkung: IBM SPSS Collaboration and Deployment Services muss so konfiguriert werden, dass es mit dem Java SDK 7 oder höher ausgeführt wird. Bei den aktuellen Fixpacks von WebSphere 8.5.5 und WebSphere 9 ist das Java SDK 8 bereits im Lieferumfang enthalten. Das Java SDK 8 ist die einzige unterstützte Version von WebSphere 9. Wenn diese Versionen von WebSphere verwendet werden, ist folglich keine zusätzliche Konfiguration für das Java SDK erforderlich.

Konfigurieren Ihres Profils für die Ausführung mit Java

Anmerkung: Da das Java SDK 8 bei den aktuellen Fixpacks von WebSphere 8.5.5 bereits im Lieferumfang enthalten ist, findet dieser Abschnitt nur auf WebSphere 8.5.5.8 oder ältere Fix-Level Anwendung.

Vor der Installation von IBM SPSS Collaboration and Deployment Services in WebSphere muss das mit IBM SPSS Collaboration and Deployment Services verwendete WebSphere-Profil so konfiguriert werden, dass es mit dem Java SDK 7 oder höher ausgeführt wird. Gehen Sie hierzu wie folgt vor:

1. Laden Sie **IBM WebSphere SDK Java Technology Edition Version 7.0** herunter und installieren Sie es in der 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, damit IBM SPSS Collaboration and Deployment Services das Java SDK 7 verwendet. Siehe http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_managesdk.html.
3. Mit WebSphere kann das SDK global (alle Profile) oder pro Profil konfiguriert werden. So legen Sie das Java SDK 7 für ein bestimmtes WebSphere-Profil fest:

   Über das Verzeichnis `<Stammverzeichnis_des_Anwendungsservers>/bin`:

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

```
C:\IBM\WebSphere\AppServer\bin> managesdk -listAvailable
                CWSDK1003I: Available SDKs :
                CWSDK1005I: SDK name: 1.6_64
```

```
                CWSDK1005I: SDK name: 1.7_64
                CWSDK1001I: Successfully performed the requested managesdk task.
```

b. Schritt 2: Legen Sie das Profil, das für IBM SPSS Collaboration and Deployment Services verwendet wird, auf das SDK der Version 7.0 fest. Beispiel:

```
C:\IBM\WebSphere\AppServer\bin>managesdk -enableProfile -profileName CADS -sdkname 1.7_64
-enableServers
                CWSDK1017I: Profile CADS now enabled to use SDK 1.7_64.
                CWSDK1001I: Successfully performed the requested managesdk task.
```

Oder alternativ zum Festlegen des Java SDK 7 für alle WebSphere-Profile (und nachfolgend erstellten Profile):

Das folgende Beispiel zeigt die Befehlsfolge, die zur Auflistung verfügbarer SDKs, zum Ändern des standardmäßigen SDKs in ein SDK der Version 7.0 und, sofern bereits Profile vorhanden sind, zum Aktivieren der Profile für die Verwendung des SDKs der Version 7.0 verwendet werden.

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

```
C:\IBM\WebSphere\AppServer\bin> managesdk -listAvailable
                CWSDK1003I: Available SDKs :
                CWSDK1005I: SDK name: 1.6_64
                CWSDK1005I: SDK name: 1.7_64
                CWSDK1001I: Successfully performed the requested managesdk task.
```

b. Schritt 2: Legen Sie die Befehlsvoreinstellung auf das SDK der Version 7.0 fest:

```
C:\IBM\WebSphere\AppServer\bin>managesdk -setCommandDefault -sdkname 1.7_64
                CWSDK1021I: The command default SDK name is now set to 1.7_64.
                CWSDK1001I: Successfully performed the requested managesdk task.
```

c. Schritt 3: Legen Sie den neuen Profilstandard auf das SDK der Version 7.0 fest:

```
C:\IBM\WebSphere\AppServer\bin>managesdk -setNewProfileDefault -sdkname 1.7_64
                CWSDK1022I: New profile creation will now use SDK name 1.7_64.
                CWSDK1001I: Successfully performed the requested managesdk task.
```

d. Schritt 4: Wenn bereits Profile vorhanden sind, aktivieren Sie die Profile für die Verwendung des SDKs der Version 7.0:

```
C:\IBM\WebSphere\AppServer\bin>managesdk -enableProfileAll -sdkname 1.7_64 -enableServers
                CWSDK1017I: Profile DEPLOYMENT now enabled to use SDK 1.7_64.
                CWSDK1001I: Successfully performed the requested managesdk task.
```

Damit föderierte Profile in einer Network Deployment-Installation geändert werden können, muss der Deployment Manager ausgeführt werden. Mit dem Befehl `managesdk` wird das Repository für die Masterkonfiguration aktualisiert. 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 eigenständigen JBoss-Server ausgeführt werden.

Vor der Installation mit JBoss

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

Anmerkung:

- Es wird empfohlen, nur eine Instanz des Servers auszuführen. Sollten mehrere Instanzen des Repositorys mit JBoss auf einem einzelnen System eingerichtet werden müssen, finden Sie in der Dokumentation zu JBoss weitere Informationen.
- Zur Vermeidung von Fehlern beim Starten des Repositorys wird empfohlen, dass der Installationspfad des JBoss Application Server keine Leerzeichen enthält. Beispiel: `c:\jboss-eap-7.1`.

- Wenn Sie JBoss in einer IPv6-Umgebung ausführen, sind weitere Konfigurationsschritte für den Application Server erforderlich. Weitere Informationen finden Sie in der Dokumentation zu Red Hat JBoss.

Liberty

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

Vor der Installation mit einem Liberty-Cluster

1. Erstellen Sie einen WebSphere Liberty-Cluster und stellen Sie sicher, dass dieser über die Lastausgleichsfunktion zugänglich ist.
2. Konfigurieren Sie die Dateiübertragung so, dass Whitelist-Einträge geschrieben werden, indem für jedes Verbundmember im Cluster folgende Einträge zu `server.xml` hinzugefügt werden:

```
<remoteFileAccess>
      <writeDir>${wlp.usr.dir}</writeDir>
      <writeDir>${server.config.dir}</writeDir>
</remoteFileAccess>
```

3. Richten Sie für den WebSphere Liberty-Cluster unter Windows RXA für Liberty-Verbundoperationen ein. Weitere Informationen zur Vorgehensweise finden Sie in der Dokumentation zu WebSphere Liberty.

Datenbank

Vor der Installation von IBM SPSS Collaboration and Deployment Services Repository muss eine Datenbank ausgeführt werden und zugänglich sein. Es ist eine Verbindung zur Datenbank erforderlich, damit die nötigen Steuertabellen und Infrastrukturen aufgebaut werden können.

Die Datenbank und das IBM SPSS Collaboration and Deployment Services Repository müssen nicht auf demselben Server installiert werden, jedoch sind einige Konfigurationsinformationen erforderlich, um die Konnektivität sicherzustellen. Während der Installation werden Sie zur Eingabe des Namens des Datenbankservers, der Portnummer, des Benutzernamens mit dem zugehörigen Kennwort und des Namens der Datenbank aufgefordert, die zum Speichern und Abrufen von Informationen verwendet werden soll.

Wichtig: Sie müssen die Datenbank vor der Installation manuell erstellen. Es kann ein beliebiger gültiger Datenbankname verwendet werden. Wenn eine zuvor erstellte Datenbank nicht vorhanden ist, wird die Installation jedoch nicht fortgesetzt.

Datenbankberechtigungen

In der folgenden Tabelle werden die allgemeinen Datenbankberechtigungen angegeben, die für einen Benutzer für die Installation, die Anwendung von Fixes, die Aktualisierung und die Ausführung des IBM SPSS Collaboration and Deployment Services Repositorys erforderlich sind:

Tabelle 1. Benutzerberechtigungen für Wartungsaufgaben für das Repository

Berechtigung	Installation, Fixpackanwendung, Migration	Laufzeit
Ändern eines beliebigen Schemas	Erforderlich	Optional
Erstellen einer Funktion	Erforderlich	Optional
Erstellen einer Prozedur	Erforderlich	Optional
Erstellen einer Tabelle	Erforderlich	Optional
Erstellen einer Ansicht	Erforderlich	Optional

Tabelle 1. Benutzerberechtigungen für Wartungsaufgaben für das Repository (Forts.)		
Berechtigung	**Installation, Fixpackanwendung, Migration**	**Laufzeit**
Erstellen einer XML-Schemasammlung	Erforderlich	Optional
Herstellen einer Verbindung	Erforderlich	Erforderlich
Löschen	Erforderlich	Erforderlich
Ausführen	Erforderlich	Erforderlich
Einfügen	Erforderlich	Erforderlich
Referenzen	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 Berechtigungen entfernt werden, bevor das Repository gestartet und ausgeführt wird. Für die Anwendung eines Fixpacks müssen diese Berechtigungen wiedereingesetzt werden.

Die genauen Namen dieser Berechtigungen variieren je nach Datenbank, und ggf. sind andere Berechtigungen erforderlich. Folgende Beispiele stellen die Berechtigungen für bestimmte Datenbanksysteme dar.

Beispiel: Db2 11.1 für Linux, Windows und UNIX

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

Anmerkung: `DBADM` stellt explizite Schemazugriffsrechte bereit, die für die Konfiguration des IBM SPSS Collaboration and Deployment Services Repositorys erforderlich sind.

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

Folgende Berechtigungen sind für die Konfiguration des IBM SPSS Collaboration and Deployment Services Repositorys mit der Oracle 12cR1-Datenbank erforderlich:

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

Folgende Berechtigungen sind für das Starten des IBM SPSS Collaboration and Deployment Services Repositorys mit der Oracle 12c-Datenbank erforderlich:

- CREATE SESSION
- ALTER SESSION
- SESSIONS_PER USER - muss auf einen Wert größer als oder gleich 100 festgelegt sein.

Db2

Db2 für Linux, UNIX und Windows

Bei Verwendung von Db2 for Linux, UNIX und Windows-Datenbank sind die Standardparameter für die Datenbankerstellung nicht ausreichend. Folgende zusätzliche Parameter muss angegeben werden:

- Codierter UTF-8-Zeichensatz
- Pufferpool mit einer Seitengröße von 8 KB (im Beispielscript *CDS8K*) für die Tabellen, die breiter als 4 KB sind
- Tabellenbereich mit 8 KB, in dem 8 KB Pufferpool verwendet werden
- Pufferpool mit 32 KB (im Beispielscript *CDSTEMP*)
- Tabellenbereich für temporäre Tabellen mit 32 KB für beliebig große Ergebnissets, die den Pufferpool mit 32 KB verwenden

Es folgt ein Beispielscript für die Erstellung einer Datenbank mit dem Namen *SPSSCDS*. Wenn Sie das Script kopieren und einfügen, sollten Sie sicherstellen, dass es genau mit der SQL übereinstimmt. Beachten Sie, dass das Script auf einen Pfad für die Datenbankdatei im UNIX-Stil verweist. Dies muss geändert werden, wenn das Script unter Windows ausgeführt werden soll. In den Software-Downloads ist das Script Teil des Dokumentationspakets.

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

Konfiguration von JMS-Nachrichtenspeichertabellen

Wenn das IBM SPSS Collaboration and Deployment Services Repository mit einem WebSphere Application Server installiert wird, wird der WebSphere JMS-Standardprovider, Service Integration Bus (SIB), so konfiguriert, dass die Repository-Datenbank als JMS-Nachrichtenspeicher verwendet wird. 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 die JMS-Nachrichtenspeichertabellen manuell erstellt werden. Wenn Sie unter z/OS mit Db2 WebSphere-JMS-Nachrichtenspeichertabellen erstellen möchten, können Sie mit dem WebSphere-Befehl *sibDDLGenerator* die DDL generieren und die DDL anschließend auf die Datenbank anwenden, um die Tabellen zu erstellen. Weitere Informationen zu *sibDDLGenerator* finden Sie in der WebSphere-Dokumentation.

Weitere Hinweise

Bei der Ausführung von Db2 auf dedizierter Hardware wird empfohlen, den Db2 Configuration Advisor für die Leistungsverwaltung der Datenbank zu verwenden. Die Erhöhung des Werts der folgenden Parameter kann sich positiv auf die Leistung auswirken:

- **IBMDEFAULTBP**. Die Pufferpoolgröße sollte entsprechend dem verfügbaren Speicher und im Hinblick auf andere Anwendungen festgelegt werden, die auf dem System ausgeführt werden.
- **NUM_IOCLEANERS**. Die Anzahl der asynchronen Seitenlöschfunktionen muss mindestens der Anzahl der Prozessoren auf dem System entsprechen.
- **NUM_IOSERVERS**. Durch die Erhöhung der Anzahl der E/A-Server wird der Vorablesezugriff optimiert.
- **LOCKLIST**. Durch die Erhöhung des Speicherplatzes für die Sperrenliste können Zeitlimitüberschreitungen und Deadlocks bei Schreiboperationen vermieden werden.
- **MAXLOCKS**. Der Prozentsatz des Parameters *LOCKLIST*, der gefüllt sein muss, bevor der Datenbankmanager eine Erhöhung vornimmt.

Wenn Db2 auf einem gemeinsam genutzten System ausgeführt wird, muss eine Änderung dieser Werte unter Berücksichtigung der verfügbaren Systemressourcen erfolgen. Die Db2-Funktion der automatischen Leistungsoptimierung sollte als Alternative für die Verwaltung der Datenbankleistung betrachtet werden.

Microsoft SQL Server

Bei Verwendung einer Microsoft SQL Server-Datenbank:

- Das Schema *DBO* muss verwendet werden.
- Ein SQL Server-Benutzer wird für die Konfiguration des Datenbankzugriffs benötigt. Die Windows-basierte Authentifizierung wird nicht unterstützt.
- IP-Adressen müssen für das IP-Netzprotokoll aktiviert sein.
- Zur Verarbeitung von nicht-lateinischen Zeichensätzen müssen entsprechende Optionen verwendet werden. So wird beispielsweise empfohlen, die Option "Kana-Zeichen (_KS) beachten" zu verwenden, um zwischen den japanischen Zeichen der Silbenschrift Hiragana und Katakana unterscheiden zu können. Weitere Informationen zur Datenbanksortierung finden Sie in der Microsoft SQL Server-Dokumentation.
- Die ausgewählte Datenbanksortierung ist unabhängig von der Groß-/Kleinschreibung (_CI).
- Die Momentaufnahmeisolation muss für die Microsoft SQL Server-Datenbank aktiviert sein. Im Folgenden finden Sie ein Beispiel für Anweisungen zur Aktivierung der Momentaufnahmeisolation:

```
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 folgende Parameter und Konfigurationen befolgt werden. Änderungen werden an den Parameterdateien `init.ora` und `spfile.ora` vorgenommen.

Tabelle 2. Oracle-Datenbankparameter

Parameter	**Einstellung**
OPEN_CURSORS	300
NLS_CHARACTERSET	AL32UTF8
NLS_NCHAR_CHARACTERSET	AL16UTF16
SESSIONS_PER USER	Gleich oder größer als 100

Anmerkung: Legen Sie bei der Erstellung der Oracle-Instanz sowohl NLS_CHARACTERSET als auch NLS_NCHAR_CHARACTERSET fest.

Tipp: Verwenden Sie Parameter wie `NLS_LANG`, `NLS_COMP` oder `NLS_SORT` bei Ihrer Oracle-Instanz, damit bei Werten für die Benutzeranmeldung die Groß-/Kleinschreibung beachtet wird. In der Oracle-Dokumentation finden Sie weitere Informationen darüber, wie Sie ermitteln, welche Parameter Ihre Anforderungen am besten erfüllen.

Oracle XDB

Bei einer Oracle-Datenbank muss Oracle XDB (XML-Datenbankfunktion) installiert sein. Sie können dies prüfen, indem Sie das Schema (Benutzerkonto) **XDB** (`SELECT * FROM ALL_USERS`) abfragen oder überprüfen, ob **RESOURCE_VIEW** vorhanden ist (`DESCRIBE RESOURCE_VIEW`). Dem Oracle-Prinzipal, der mit dem IBM SPSS Collaboration and Deployment Services Repository verwendet wird, muss die Rolle **XDBADMIN** erteilt werden.

Fehler bei der Migration von Daten von 12c zu 19c

Beachten Sie beim Upgrade von 12c auf 19c, dass folgende neun Benutzerrollennamen aus 12c in 19c nicht mehr vorhanden sind:

- XS_RESOURCE
- JAVA_DEPLOY
- SPATIAL_WFS_ADMIN
- WFS_USR_ROLE
- SPATIAL_CSW_ADMIN
- CSW_USR_ROLE
- APEX_ADMINISTRATOR_ROLE
- APEX_GRANTS_FOR_NEW_USERS_ROLE
- DELETE_CATALOG_ROLE

Wenn Sie diese Rollen in 12c verwendet haben, werden Ihnen beim Importieren von Daten in 19c folgende Fehler angezeigt:

```
ORA-39083: Object type ROLE_GRANT failed to create with error:
ORA-01919: role 'XXX' does not exist
Failing sql is:
 GRANT "XXX" TO "%schemaName%" WITH ADMIN OPTION
```

Da sich einige Rollennamen in 19c geändert haben, sollte Ihr Datenbankadministrator sicherstellen, dass vor dem Import entsprechende neue Rollenberechtigungen manuell erteilt werden. Auf diese Weise wird verhindert, dass diese Fehler die Installation und Verwendung von IBM SPSS Collaboration and Deployment Services beeinträchtigen.

Wartung der Repository-Datenbank

Es wird dringend empfohlen, die Wartungsaufgaben der IBM SPSS Collaboration and Deployment Services Repository-Datenbank in regelmäßigen Intervallen durchzuführen.

Tabelle 3. Wartungsplanung für die Repository-Datenbank

Aufgabe	**Empfohlener Zeitplan**
Backup	Täglich
Statistikdaten aktualisieren	Täglich
Konsistenzprüfung	Wöchentlich
Reorganisieren	Wöchentlich
Erneut erstellen	Monatlich

Aktivieren benutzerdefinierter JDBC-URL-Einstellungen

1. Erstellen Sie auf Ihrem lokalen System eine neue Eigenschaftendatei und fügen Sie dieser Ihre benutzerdefinierte JDBC-URL hinzu. Erstellen Sie beispielsweise die Datei `C:\temp\db.properties` und fügen Sie dieser folgende URL-Einstellung hinzu:

   ```
   db2_url=spss:jdbc:spssoem:db2://${host}:${port};DatabaseName=${name};LobStreamingProtocol=ma
   terialize;DynamicSections=400;CreateDefaultPackage=TRUE;AuthenticationMethod=encryptedUID
   Password;ReplacePackage=TRUE%{;EncryptionMethod=SSL}
   ```

   Hinweise:

   - In der Eigenschaftendatei ist eine Zeile zulässig (da es nur eine Datenbank als Installationsziel gibt).
   - Für den Eigenschaftsnamen müssen Sie einen der folgenden Werte verwenden: `sqlserver_url`, `oracle_sid_url`, `oracle_service_url`, `db2_url` oder `db2zos_url`.
   - Für den Eigenschaftswert müssen Sie eine JDBC-Verbindungs-URL verwenden, die auf der IBM SPSS Collaboration and Deployment Services-Standardeinstellung basiert (siehe folgendes Aufzählungszeichen). Sie muss eines der folgenden Element enthalten: `url.contains("%{;EncryptionMethod=SSL}") && url.contains("${host}") && url.contains("${port}") && url.contains("${name}")`.
   - Die standardmäßige JDBC-URL für IBM SPSS Collaboration and Deployment Services lautet wie folgt:

     ```
     sqlserver_url=spss:jdbc:spssoem:sqlserver://${host}:${port};DatabaseName=${name};SelectMe
     thod=cursor;MaxPooledStatements=250;allowPortWithNamedInstance=true%{;EncryptionMethod=SSL}
     db2_url=spss:jdbc:spssoem:db2://${host}:${port};DatabaseName=${name};LobStreamingProto
     col=materialize;DynamicSections=400;BatchPerformanceWorkaround=TRUE%{;EncryptionMethod=SSL}
     oracle_sid_url=spss:jdbc:spssoem:oracle://${host}:${port};SID=${name}%{;EncryptionMe
     thod=SSL}
     oracle_service_url=spss:jdbc:spssoem:oracle://${host}:${port};ServiceName=${name}%{;Encryp
     tionMethod=SSL}
     db2zos_url=spss:jdbc:spssoem:db2://${host}:${port};LocationName=${name};LobStreamingProto
     col=materialize;QueryBlockSize=1;ConcurrentAccessResolution=useCurrentlyCommitted;AddToC
     reateTable=CCSID UNICODE;BatchPerformanceWorkaround=TRUE%{;EncryptionMethod=SSL}
     ```

2. Bearbeiten Sie vor dem Starten von Installation Manager die Datei `IBMIM.ini` im Verzeichnis `[Install Manager Install Dir]/eclipse`. Fügen Sie eine neue Zeile hinzu, die auf die Eigenschaftendatei verweist, die Sie in Schritt 1 erstellt haben:

   ```
   -Dcads.jdbc.config.file=D:\temp\db.properties
   ```

3. Wenn Sie nun Installation Manager starten und mit der IBM SPSS Collaboration and Deployment Services-Installation beginnen, werden beim Installationsprozess Ihre benutzerdefinierten JDBC-URL-Einstellungen verwendet.

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

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

Das Konfigurationsdienstprogramm für das IBM SPSS Collaboration and Deployment Services Repository führt folgende Aufgaben aus:

- Es erstellt Datenbankobjekte für das Content-Repository
- Es erstelle Anwendungsserverressourcen, z. B. JMS-Warteschlangen, und stellt auf dem Anwendungserver Java-Programme bereit
- Es konfiguriert Verschlüsselung und Sicherheit

Während es sich bei der Konfiguration mit einem eigenständigen Anwendungsserver um den letzten nötigen Installationsschritt handelt, sind in einer Clusterumgebung weitere Schritte erforderlich. Weitere Informationen finden Sie im Thema „Clusterkonfiguration” auf Seite 24.

Vor Installation und Konfiguration

1. Überprüfen Sie, ob der Anwendungsserver installiert wurde und funktioniert. Wenn Sie eine automatische Konfiguration durchführen (Konfiguration, bei der die Artefakte erstellt und diese auf dem Anwendungsserver bereitgestellt werden), muss der Anwendungsserver den folgenden Status aufweisen:
   - **WebSphere eigenständig:** Server muss beendet werden.
   - **WebSphere verwaltet:** Der verwaltete Server muss beendet und der Deployment Manager-Server ausgeführt werden.
   - **WebSphere-Cluster:** Clustermitglieder müssen gestoppt und der Deployment Manager-Server ausgeführt werden.
   - **JBoss:** Der Server muss beendet werden.
   - **Liberty eigenständig:** Es sind keine weiteren Maßnahmen erforderlich.

- **Liberty-Cluster:** Sowohl Verbundcontroller als auch Clustermitglieder müssen gestoppt werden. Die für den Repository-Server erforderlichen Funktionen müssen auf dem Controller-Server und dem Member-Server installiert werden.

```
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. Überprüfen Sie, ob auf die Datenbank zugegriffen werden kann.
3. Wenn Sie eine vorhandene Repository-Datenbank mit WebSphere wiederverwenden, löschen Sie den SIB (JMS-Nachrichtenspeichertabellen).

Installations- und Konfigurationsschritte

1. Melden Sie sich als Benutzer mit entsprechender Berechtigungsstufe beim Betriebssystem an. Weitere Informationen finden Sie im Thema „Benutzer- und Dateisystemberechtigungen” auf Seite 9.
2. Starten Sie IBM Installation Manager:

   GUI-Modus:

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

   Befehlszeilenmodus:

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

3. Geben Sie den Repository-Pfad an (z. B. in Form einer Position auf dem Hostdateisystem, des Netzes oder einer HTTP-Adresse), wenn das Installationsrepository nicht konfiguriert ist.

   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 Paket aus, das installiert werden soll.

   Anmerkung: Sie können auch Adapter oder Komponenten auswählen, die mit dem IBM SPSS Collaboration and Deployment Services-Server installiert werden sollen, wie z. B. den IBM SPSS Collaboration and Deployment Services Scoring Adapter for PMML. Voraussetzung hierfür ist, dass diese Adapter oder Komponenten in den In stallationsrepositorys verfügbar sind.
5. Lesen Sie die Lizenzvereinbarung und akzeptieren Sie deren Bedingungen.
6. Geben Sie die Paketgruppe und das Installationsverzeichnis an.
   - Für die IBM SPSS Collaboration and Deployment Services Repository-Installation ist eine neue Paketgruppe erforderlich.

- Geben Sie das Installationsverzeichnis für gemeinsam genutzte Ressourcen an. Sie können das Verzeichnis für gemeinsam genutzte Ressourcen nur bei der Erstinstallation 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 Anwendungsservereinstellungen an:
   - WebSphere
     - **WebSphere-Profilstammverzeichnis.** Die Verzeichnisposition des WebSphere-Serverprofils. Beachten Sie, dass es sich bei einem verwalteten Server oder Cluster um den Pfad des Deployment Manager-Profils handelt.
     - **WebSphere-Installationsstammverzeichnis.** Die Verzeichnisposition, an der der WebSphere-Server installiert ist.
     - **Servertopologie.** WebSphere-Profiltopologie: eigenständig, verwaltet oder Cluster. Sie müssen eine Topologie auswählen, wenn das Deployment Manager-Profil sowohl verwaltete Server als auch Cluster enthält.
     - **URL-Präfix.** Bei einer Clusterinstallation die URL der Lastausgleichsfunktion oder des Proxy-Servers für die Weiterleitung der vom Server initiierten Anforderungen.
     - **WebSphere-Server oder -Cluster.** 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 ist dies der Knotennamen des dmgr-Knotens.
     - **JVM.** Die Verzeichnisposition der WebSphere-JVM, die vom Zielprofil verwendet wird.
     - **WebSphere-Benutzername und -Kennwort.** Nur wenn die Verwaltungssicherheit aktiviert ist.
   - JBoss
     - **Serververzeichnispfad.** Die Verzeichnisposition, an der JBoss installiert ist.
     - **JBoss-Server.** Der Name des JBoss-Servers. Geben Sie den Wert `standalone` an.
     - **JVM.** Die Verzeichnisposition der 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*, es sei denn, die Servereigenschaften (z. B. Bindungsadresse oder Port) wurden geändert. Beachten Sie, dass *localhost* nicht als Teil des URL-Präfixes zulässig ist. Der Präfixwert muss extern auflösbar sein, wenn externe Clients eine Verbindung zum IBM SPSS Collaboration and Deployment Services Repository herstellen.
   - Liberty
     - **Eigenständig.** Das WebSphere Liberty-Profil ist im Lieferumfang des IBM SPSS Collaboration and Deployment Services Repository-Servers enthalten. Wählen Sie diese Option aus, wenn Sie mit dem Repository-Server ein neues Liberty-Profil installieren möchten.
     - **Cluster.** Wählen Sie diese Option aus, wenn Sie den IBM SPSS Collaboration and Deployment Services Repository-Server in einem vorhandenen Liberty-Cluster installieren möchten.

       Folgende Konfigurationsoptionen sind nur verfügbar, wenn **Cluster** ausgewählt wurde:

       - Host des Verbundcontrollers (Hostname oder IP). Der Hostname oder die IP-Adresse, unter dem bzw. der der Verbundcontroller eingerichtet wird.
       - Port des Verbundcontrollers. Der sichere HTTPS-Port des Verbundcontrollers, der in der Datei `server.xml` definiert ist.
       - Benutzername des Administrators des Verbundcontrollers. Der Benutzername für das Administrationskonto des Verbundcontrollers.

- Administratorkennwort für den Verbundcontroller. Das Kennwort für das Administrationskonto des Verbundcontrollers.
- Truststore-Datei des Verbundcontrollers. Die Position der Truststore-Datei des Verbundcontrollers mit dem Namen `collectiveTrust.p12`. Diese Datei kann sich auf dem lokalen Dateisystem befinden oder von einem anderen Dateisystem kopiert werden. Beachten Sie, dass der Standardkeystoretyp in Liberty 19.0.0.3 von JKS in PKCS12 geändert wurde. Wenn ein Liberty-Server eine Konfiguration aufweist, bei der eine JKS-Keystore-Datei verwendet wird, müssen Sie diese in das PKCS12-Format umwandeln. Weitere Informationen zum Umwandeln der Keystore-Datei finden Sie unter https://www.ibm.com/support/knowledgecenter/SS7K4U_liberty/com.ibm.websphere.wlp.zseries.doc/ae/rwlp_liberty_keystore_default.html.
- Kennwort für die Truststore-Datei des Verbundcontrollers. Das Kennwort für die Truststore-Datei des Verbundcontrollers.
- URL-Präfix. Dies ist die URL für die Weiterleitung der vom Server initiierten Anforderungen. In den meisten Fällen handelt es sich hierbei um den Port der Lastausgleichsfunktion für das Cluster-Setup.
- Cluster erkennen. Klicken Sie auf **Cluster erkennen**, nachdem Sie sämtliche Informationen zum Liberty-Verbundcontroller eingegeben haben. Es werden alle verfügbaren Cluster aufgeführt, die auf dem Server des Verbundcontrollers vorkonfiguriert wurden. Anschließend können Sie den Cluster auswählen, in dem Sie den IBM SPSS Collaboration and Deployment Services Repository-Server installieren möchten.

9. Geben Sie Datenbankverbindungsinformationen an:
   - **Datenbanktyp.** IBM Db2, SQL Server oder Oracle.
   - **Host.** Der Hostname oder die Adresse des Datenbankservers.
   - **Port.** Der Zugriffsport für den Datenbankserver.
   - **Datenbankname.** Der Name der Datenbank, die für das Content-Repository verwendet werden soll.
   - **Quellen-ID/Servicename.** Bei Oracle die Quellen-ID oder der Servicename.
   - **Als Service ausführen.** Gibt bei Oracle an, dass die Verbindung zu einem Datenbankservice besteht und nicht über die Quellen-ID hergestellt wurde.
   - **Benutzername.** Der Datenbankbenutzername.
   - **Kennwort.** Das Kennwort des Datenbankbenutzers.
10. Geben Sie bei der Wiederverwendung einer Datenbank aus einer vorherigen Installation an, ob vorhandene Daten beibehalten oder verworfen werden sollen.
11. Geben Sie die Optionen für den Keystore für Verschlüsselungsschlüssel an. Bei dem Keystore handelt es sich um eine verschlüsselte Datei, die den Schlüssel zum Entschlüsseln der Kennwörter enthält, die vom Repository verwendet werden (z. B. das Kennwort für die Repository-Verwaltung, das Kennwort für den Datenbankzugriff usw.).
    - Geben Sie zur Wiederverwendung eines Keystores aus einer vorhandenen Repository-Installation den Pfad und das Kennwort für den Keystore an. Der Schlüssel aus dem alten Keystore wird extrahiert und im neuen Keystore verwendet. Beachten Sie, dass die JRE, die zur Ausführung des Anwendungsservers verwendet wird, mit der JRE kompatibel sein muss, die zum Erstellen der Verschlüsselungsschlüssel verwendet wurde.
    - Wenn Sie einen vorhandenen Keystore nicht wiederverwenden, geben Sie das Kennwort für den neuen Keystore an und bestätigen Sie dieses. Der Keystore wird unter *<Repository-Installationsverzeichnis>/keystore* erstellt.

    Wichtig: Wenn die Keystore-Datei verloren geht, ist die Anwendung nicht in der Lage, Kennwörter zu entschlüsseln, und kann nicht mehr verwendet werden. Sie muss folglich erneut installiert werden. Daher wird empfohlen, die Sicherungskopien der Keystore-Datei zu speichern.
12. Geben Sie den Kennwortwert an, der für das Benutzerkonto des Administrators (*admin*) für das integrierte Repository verwendet werden soll. Das Kennwort wird bei der ersten Anmeldung beim Repository verwendet.

13. So 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 und Installationsscripts im Ausgabeverzeichnis *toDeploy/<Zeitmarke>* generiert. Diese Artefakte können später zur manuellen Bereitstellung des Repositorys verwendet werden. Die manuelle Konfiguration ist für fortgeschrittene Benutzer vorgesehen, wenn mehr Kontrolle über die Anwendungsserverumgebung erforderlich ist.
14. Prüfen Sie die Übersichtsinformationen und fahren Sie mit der Installation fort. Wählen Sie im Hauptmenü **Installieren** aus. Die Anwendungsdateien werden im angegebenen Verzeichnis installiert.

- Wenn die Konfiguration erfolgreich war, können Sie mit den Schritten nach der Installation fortfahren, wie z. B. dem Starten des Repositorys und dem 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.
- Wenn Sie das Repository mit einem Cluster von Anwendungsservern installieren, können Sie mit der Konfiguration der anderen Clusterknoten fortfahren. Weitere Informationen finden Sie im Thema „Clusterkonfiguration” auf Seite 24.

Anmerkung: Die Konfigurationsoperation kann 15-30 Minuten oder länger dauern. Dies hängt von Ihrer Hardware, der Netzgeschwindigkeit, der Komplexität Ihrer Andwendungsservertopologie usw. ab. Wenn der Konfigurationsprozess nicht zu antworten scheint oder ein Fehler gemeldet wird, sollten Sie die Protokolldateien unter *<IBM SPSS Collaboration and Deployment Services Repository-Installationsverzeichnis>/log* prüfen.

Unbeaufsichtigte Konfiguration

Die IBM SPSS Collaboration and Deployment Services Repository-Konfiguration 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 für eine 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 8.3.0' installLocation='/opt/IBM/
SPSS/Deployment/8.3.0/Server'>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='user.LibertyTopologyUserData,com.ibm.spss.cds.server.v8.3.0.offering' va□
lue='single'/>
    <data key='user.KeyPassUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
    <data key='user.ReuseKeyUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='false'/>
    <data key='user.KeyPwdUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
    <data key='user.AdminPassUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
    <data key='user.AdminPwdUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
    <data key='user.DBPort,com.ibm.spss.cds.server.v8.3.0.offering' value='50000'/>
    <data key='user.DBName,com.ibm.spss.cds.server.v8.3.0.offering' value='cadsdb'/>
    <data key='user.DBHost,com.ibm.spss.cds.server.v8.3.0.offering' value='x.x.x.x'/>
    <data key='user.DBTypeUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='db2'/>
    <data key='user.DataEraseUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='false'/>
    <data key='user.DBPassword,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
    <data key='user.SSLServiceUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='false'/>
    <data key='user.OracleServiceUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='fal□
se'/>
    <data key='user.DBUsername,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
    <data key='user.DeployOptionUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='automa□
tic deployment'/>

  </profile>
  <install>
```

```
    <!-- IBM SPSS Collaboration and Deployment Services - Repository Server 8.3.0.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.3.0'
id='com.ibm.spss.cds.server.v8.3.0.offering' features='deploy.liberty'/>
    <!-- IBM SPSS Modeler Adapters for Collaboration and Deployment Services 18.3.0.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.3.0'
id='com.ibm.spss.modeler.adapter.18.3.0' features='main.feature,text.analytics'/>
    <!-- IBM SPSS PMML Scoring Adapter 8.3.0.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.3.0'
id='com.ibm.spss.pmml.scoring.adapter.v8.3.0' features='main.feature'/>
  </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 Clusteranwendungsservern bereitgestellt werden. Jeder Anwendungsserver im Cluster sollte die identische Konfiguration für die gehosteten Anwendungskomponenten aufweisen. Der Zugriff auf das Repository erfolgt über eine hardware- oder softwarebasierte Lastausgleichsfunktion. Durch diese Architektur wird eine Verteilung der Verarbeitung auf mehrere Anwendungsserver ermöglicht. Zudem bietet sie Redundanz im Falle eines Serverfehlers.

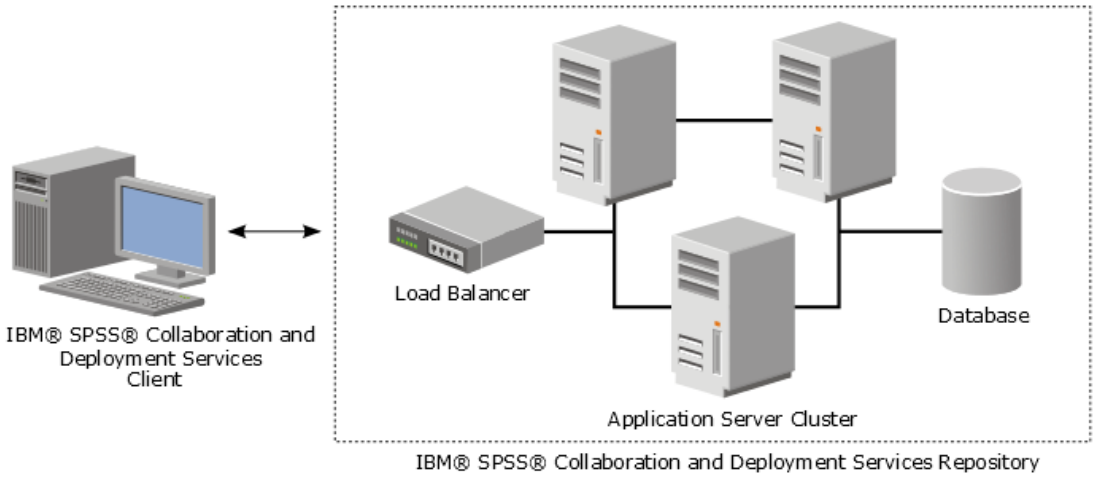

Abbildung 2. Architektur einer Clusterbereitstellung

Die Installation des Repositorys in einem Cluster umfasst die folgenden Schritte:

- Erstinstallation und -konfiguration der Anwendungskomponenten auf dem Managementknoten des Clusters.
- Anschließende Konfiguration der Clusterknoten.

Das IBM SPSS Collaboration and Deployment Services Repository unterstützt derzeit das Clustering von herkömmlichen WebSphere-Anwendungsservern und WebSphere Liberty-Profilen. Befolgen Sie die anwendungsserverspezifischen Anweisungen, um die Bereitstellung abzuschließen.

Installationsvoraussetzungen

- Die Hostsystemanforderungen müssen auf allen Knoten des Clusters erfüllt sein.
- Alle IBM SPSS Collaboration and Deployment Services Repository-Clustermember müssen unter demselben Betriebssystem als Hauptknoten (Managementknoten) ausgeführt werden.
- Die Repository-Datenbank muss bereits vorhanden und zugänglich sein.

- Die Topologie des Anwendungsservers muss bereits vor der Installation des IBM SPSS Collaboration and Deployment Services Repositorys vorhanden sein. Es wird empfohlen, zu prüfen, ob der Cluster zugänglich ist und an der Adresse der Lastausgleichsfunktion ordnungsgemäß ausgeführt wird.
- Das IBM SPSS Collaboration and Deployment Services Repository-Installationsverzeichnis muss im Cluster knotenübergreifend gemeinsam genutzt werden.

WebSphere-Cluster

1. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind.
2. Führen Sie die Installation und die Konfiguration durch. Sie können auswählen, ob die Anwendung automatisch oder manuell bereitgestellt wird. Weitere Informationen finden Sie im Thema „Installation und Konfiguration” auf Seite 19.
3. Konfigurieren Sie das freizugebende Installationsverzeichnis so, dass alle Mitglieder im Cluster darauf zugreifen können.
4. Legen Sie den Wert der Variablen **CDS_HOME** für jeden 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.configurationFile** 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://${CDS_HOME}/platform/log4j2.xml`.
   - Öffnen Sie die Administrationskonsole.
   - Prüfen Sie für jeden Server im Cluster den Wert **log4j.configurationFile**. Dieser Wert ist über **Anwendungsserver** > ***Servername*** > **Prozessdefinition** > **Java Virtual Machine** > **Benutzerdefinierte Eigenschaften** verfügbar, wobei *Servername* dem jeweiligen Server entspricht.
   - Wenn auf dem Windows-Betriebssystem die Variable **CDS_HOME** aus dem Schritt „4” auf Seite 25 einen Laufwerkbuchstaben enthält, fügen Sie dem Wert **log4j2.xml** als Escapezeichen einen Schrägstrich ("/") hinzu. Der neue Wert würde dann beispielsweise wie folgt lauten: `file:////$ {CDS_HOME}/platform/log4j2.xml`.
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 „Lastausgleichskonfiguration” auf Seite 25.
8. Starten Sie den WebSphere-Cluster.

Lastausgleichskonfiguration

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 in „Installation und Konfiguration” auf Seite 19.

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 hohen Verarbeitungslasten, muss der Cluster, der das IBM SPSS Collaboration and Deployment Services Repository ausführt, möglicherweise erweitert werden, indem nach der Erstinstallation Knoten hinzugefügt werden.

WebSphere

1. Erstellen Sie weitere, von WebSphere verwaltete Profile und binden Sie diese in die Zelle ein. Erstellen Sie Server und fügen Sie diese über die WebSphere-Konsole dem Cluster hinzu.
2. Führen Sie das Script *CrtCDSresources.py* im Verzeichnis */toDeploy/* aus, um den bzw. die neuen Knoten zu aktualisieren, der bzw. die für die Zelle definiert wurden.

   ```
   /bin/wsadmin -lang jython -f CrtCDSresources.py -update
   ```

3. Legen Sie den Wert der Variablen *CDS_HOME* für jeden Knoten fest. Weitere Informationen finden Sie in „WebSphere-Cluster” auf Seite 25.
4. Starten Sie den Cluster erneut.

Nach der Installation

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

- Starten Sie den Server und prüfen Sie die Konnektivität. Konfigurieren Sie ggf. den automatischen Start des Servers.
- Installieren Sie einen beliebigen Inhaltsadapter für die Verwendung des IBM SPSS Collaboration and Deployment Services Repositorys mit anderen IBM SPSS-Produkten, wie z. B. IBM SPSS Statistics und IBM SPSS Modeler.
- 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 unter *Installationsanweisungen zu IBM SPSS Collaboration and Deployment Services Remote Process Server 8.3.0* und *Installationsanweisungen zu IBM SPSS Collaboration and Deployment Services - Essentials for Python 8.3.0*.
- Ändern Sie bei Bedarf das Kennwort für die Masterdatenbank.
- Installieren Sie bei Bedarf zusätzliche JDBC-Treiber.
- Installieren Sie IBM SPSS Collaboration and Deployment Services-Clients und IBM SPSS Deployment Manager. Weitere Informationen finden Sie in den Installationsanweisungen zur Clientanwendung.
- Erstellen Sie mithilfe von 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 8.3.0*.

Sollten in den Schritten nach der Installation Probleme auftreten, finden Sie im *Handbuch zur Fehlerbehebung zu IBM SPSS Collaboration and Deployment Services 8.3.0* weitere Informationen.

Starten des Repository-Servers

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

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

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

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

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

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

WebSphere

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

WebSphere Liberty-Standalone-Server

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

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

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

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

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

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

WebSphere Liberty-Cluster

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

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

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

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

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

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

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

JBoss

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

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

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

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

Prüfen der Konnektivität

Sie können prüfen, ob das IBM SPSS Collaboration and Deployment Services Repository ausgeführt wird, indem Sie über einen 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 für den Administrator an. Die Berechtigungsnachweise werden während der Repository-Konfiguration festgelegt.

Verwalten des Datenbankkennworts

Das Datenbankkennwort, das bei der Konfiguration des IBM SPSS Collaboration and Deployment Services Repositorys bereitgestellt wird, wird als Teil der Datenquellendefinition in den Einstellungen für den Anwendungsserver gespeichert. Ggf. sind weitere Schritte erforderlich, damit die Sicherheit des Datenbankkennworts gewährleistet ist.

Testen der Datenbankverbindung

Die Verbindung der IBM SPSS Collaboration and Deployment Services Repository-Datenbank kann mithilfe der Funktionen für die Datenquellenverwaltung auf der Administrationskonsole des Anwendungsservers getestet werden.

Anwendungsserver	Name des Datenquellenobjekts
WebSphere Traditional	CDS_DataSource
WebSphere Liberty	CDS_DataSource
JBoss	jdbc/spss/PlatformDS

JAAS-Objektsicherheit

Die Berechtigungsnachweise für die IBM SPSS Collaboration and Deployment Services-Datenquelle, die auf dem Anwendungsserver erstellt wurden, bleiben als JAAS-Objekt erhalten.

Wichtig: Wenn das Repository auf dem WebSphere-Anwendungsserver entweder über die automatische Bereitstellung (mit IBM Installation Manager) oder mit Scripts konfiguriert wird, die von dem Konfigurationsdienstprogramm generiert werden, wird das Kennwort als Klartext an den Anwendungsserver übergeben und bleibt dann gemäß den Anwendungsservereinstellung erhalten. Obwohl die WebSphere-Standardeinstellungen das Speichern von Kennwörtern in verschlüsselter Form vorsehen, muss ggf. sichergestellt werden, dass das Kennwort nicht als Klartext gespeichert wird. In der Anwendungsserverdokumentation finden Sie weitere Informationen zum Kennwortschutz.

Ändern des Datenbankkennworts

Aus Sicherheitsgründen muss das Datenbankkennwort nach der Installation des IBM SPSS Collaboration and Deployment Services Repositorys ggf. geändert werden. In solchen Fällen kann das gespeicherte Datenbankkennwort mit dem IBM SPSS Collaboration and Deployment Services Password Utility geändert werden.

So führen Sie das Dienstprogramm für Kennwörter aus:

1. Fahren Sie den Anwendungsserver herunter, der IBM SPSS Collaboration and Deployment Services hostet.
2. Führen Sie

   Windows aus:

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

   UNIX:

   ```
   <Repository-Installationsverzeichnis>/bin/cliUpdateDBPassword.sh
   ```
3. Starten Sie den Anwendungsserver, der IBM SPSS Collaboration and Deployment Services hostet.
4. Geben Sie über die Eingabeaufforderung das Kennwort an und bestätigen Sie dieses.

Das Kennwort kann auch durch Ändern der Anwendungsservereinstellungen geändert werden. Beachten Sie, dass das Kennwort in verschlüsselter Form gespeichert wird. Daher kann das neue Kennwort in eine verschlüsselte Zeichenfolge umgewandelt werden, indem `cliEncrypt.bat`/`cliEncrypt.sh` mit dem Kennwort als Befehlszeilenargument ausgeführt wird.

JDBC-Treiber

Hinzufügen von Treiberunterstützung zum IBM SPSS Collaboration and Deployment Services Repository

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

Wenn IBM SPSS Collaboration and Deployment Services keinen Treiber für eine erforderliche Datenbank enthält, können Sie Ihre Umgebung aktualisieren, damit ein Treiber eines anderen Herstellers für die Datenbank aufgenommen wird. Treiber von anderen Herstellern können verwendet werden, indem Sie Ihre Repository-Installation durch die Treiberdateien erweitern.

Abhängig vom Anwendungsserver lautet die Verzeichnisposition der JDBC-Treiber wie folgt:

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

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

Beachten Sie, dass bei Netezza der Treiber der Version 5.0 verwendet werden sollte, damit auf die Datenbanken der Versionen 4.5 und 5.0 zugegriffen werden kann.

Hinzufügen von Treiberunterstützung zu Clientanwendungen

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

1. Schließen Sie die Clientanwendung, falls sie ausgeführt wird.
2. Erstellen Sie auf der Stammverzeichnisebene des Clientinstallationsverzeichnisses einen Ordner namens `JDBC`.
3. Platzieren Sie die Treiberdateien in dem Ordner `JDBC`

Nachdem Sie Ihrer Umgebung die Treiberdateien hinzugefügt haben, kann der Treiber in einer Datenquellendefinition verwendet werden. Geben Sie in das Dialogfeld "JDBC-Name und URL" den Namen und die URL für den Treiber ein. Befolgen Sie die Anweisungen in der Herstellerdokumentation, damit der Treiber den korrekten Klassennamen und das korrekte URL-Format erhält.

IBM SPSS-Produktkompatibilität

Die Funktionalität des IBM SPSS Collaboration and Deployment Services Repositorys kann erweitert werden, damit andere Anwendungen von IBM SPSS unterstützt werden, indem zusätzliche Inhaltsadapterpakete installiert werden.

Informationen zu den aktuellen Kompatibilitätsinformationen 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.

Anmerkung:

- Bei einigen Produkten müssen ggf. Patches angewendet werden. Informieren Sie sich bei dem IBM Corp. Support, um das richtige Patch-Level in Erfahrung zu bringen.
- Sie müssen überprüfen, ob die Installations- und Laufzeitanforderungen für Anwendungen von IBM SPSS (z. B. Anwendungsserver und Datenbanken) mit den Anforderungen für das IBM SPSS Collaboration and Deployment Services Repository kompatibel sind. Ausführliche Informationen finden Sie in den Berichten zur Kompatibilität von Softwareprodukten und in der Dokumentation zu einzelnen Produkten von IBM SPSS.

Der IBM SPSS Statistics-Client und der IBM SPSS Modeler-Client sind für die Verwendung von IBM SPSS Collaboration and Deployment Services nicht erforderlich. Diese Anwendungen bieten jedoch Schnittstellen zur Verwendung des IBM SPSS Collaboration and Deployment Services Repositorys, um Objekte zu

speichern und abzurufen. Die Serverversionen dieser Produkte sind für Jobs erforderlich, die IBM SPSS Statistics- oder IBM SPSS Modeler-Objekte enthalten, die auszuführen sind.

Das Repository wird standardmäßig ohne Adapter für andere Produkte von IBM SPSS installiert. Darüber hinaus müssen Benutzer die Adapterpakete installieren, die ihren Produktversionen entsprechen. Die Pakete sind auf dem Verteilerdatenträger des jeweiligen Produkts enthalten.

Beachten Sie, dass Sie erst dann IBM SPSS-Produktobjekte im Repository speichern sollten, nachdem Sie die erforderlichen Adapterpakete installiert haben. Wenn Sie dies tun, wird das Objekt selbst nach der Installation der Adapterpakete als Typ nicht erkannt. Sie müssen die Objekte dann löschen und dem Repository erneut hinzufügen. Wenn z. B. im Repository ein IBM SPSS Modeler-Stream gespeichert wird, bevor der IBM SPSS Modeler-Adapter installiert wird, wird der MIME-Typ nicht erkannt und stattdessen als generischer Typ festgelegt. Dies führt dazu, dass die Stream-Datei unbrauchbar ist.

Für Docker vorbereitete Installation

Zwecks einfacherer Bereitstellung ist eine für Docker vorbereitete Installation des Repository-Servers verfügbar. Sie können das vordefinierte IBM SPSS Collaboration and Deployment Services-Image laden. In einem zukünftigen Release wird eine vollständig funktionsfähige, Docker-basierte Clusterunterstützung hinzugefügt, die Ihnen Hochverfügbarkeit, Lastausgleich usw. bietet.

Das für Docker vorbereitete IBM SPSS Collaboration and Deployment ServicesBereitstellungspaket kann in verschiedenen Docker-Umgebungen ausgeführt werden und stellt den vollständigen Repository-Server bereit, der über eine Containermethode funktioniert.

Voraussetzungen

Wenn Sie den für Docker vorbereiteten Repository-Server ausführen möchten, sollten Sie sicherstellen, dass Sie die folgenden Voraussetzungen erfüllen.

- Die Docker-Engine muss unter dem Zielbetriebssystem ordnungsgemäß installiert und konfiguriert werden. Weitere Informationen finden Sie in der Herstellerdokumentation zu Docker. Unterstützte Betriebssysteme sind Windows x64, RedHat x64 und Ubuntu x64.
- Der Docker-Dämon muss sich im Laufstatus befinden.
- Bei der Docker-Engine, die unter Windows x64 gehostet wird, muss der Docker-Dämon im Modus *Linux-Container* ausgeführt werden.
- Stellen Sie sicher, dass mindestens 20 GB freier Plattenspeicherplatz vorhanden sind, damit das Docker-Image für den Repository-Server geladen werden kann.
- Stellen Sie sicher, dass Sie eine IBM SPSS Collaboration and Deployment Services-Datenbank vorbereitet haben, entweder über eine neue Datenbank initialisiert, aus einem früheren Release migriert oder aus einer anderen Instanz einer aktiven IBM SPSS Collaboration and Deployment Services-Datenbank. Weitere Informationen zur Initialisierung und Migration von Repository-Datenbanken finden Sie weiter unten in diesem Abschnitt unter **Vorbereitung für Docker**.

Typischer Anwendungsfall

1. Führen Sie das IBM SPSS Collaboration and Deployment Services Dockerize Preparation Toolkit aus, um eine neue Datenbank zu initialisieren oder eine Migration aus einer Repository-Datenbank der Version 8.1.1 durchzuführen. Details finden Sie im folgenden Abschnitt **Vorbereitung für Docker**.
2. Laden Sie das IBM SPSS Collaboration and Deployment Services-Docker-Paket (`.zip`-Datei) von Passport Advantage herunter und extrahieren Sie es in das lokale Dateisystem.
3. Erstellen Sie in dem dekomprimierten Ordner aus Schritt 2 eine Kopie des Ordners `keystore`, der in Schritt 1 generiert bzw. wiederverwendet wird.
4. Bearbeiten Sie die Datei `cads_db.env` mit Ihren Informationen zur Repository-Datenbank. Diese Datei weist folgende Inhalte auf:

```
#CaDS Repository Database configuration file. Enter your database information.
#Examples:
```

```
#DB_TYPE=db2
#DB_HOST=8.8.8.8
#DB_PORT=50000
#DB_NAME=cadsdb
#DB_USERNAME=dbuser
#Additional Notes:
#DB_TYPE can be db2, sqlserver, oracle_sid, db2zos, or oracle_service
DB_TYPE=
DB_HOST=
DB_PORT=
DB_NAME=
DB_USERNAME=
```

5. Führen Sie abhängig von Ihrem Betriebssystem `cdsServer.sh` oder `cdsServer.bat` aus, um Operationen durchzuführen, wie z. B. die Überprüfung der Umgebung und das Laden des Image- und Startcontainers. Die ausführliche Syntax lautet wie folgt:

```
./cdsServer.sh

This script intends to provide full management functionalities to Dockerized IBM SPSS Colla
boration and Deployment Services Repository Server (aka. CaDS)

Usage: cdsServer check | load | start --port --db_pass | list | stop --container_id | remove
| help

check
    check the availability of docker engine

load
    load CaDS docker image tarball to local

start --port --db_pass
    start CaDS container and specify the port which container is exposed to, need to input
the repository database password to connect

list
    list all the containers of CaDS

stop --container_id | --all
    stop all CaDS containers or specified by the container id

remove
    remove all the stopped CaDS containers

help
    print all the command usage
```

Vorbereitung für Docker

Mithilfe des IBM SPSS Collaboration and Deployment Services Dockerize Preparation Toolkits können Sie eine vorbereitete Repository-Datenbank für die Verwendung mit dem für Docker vorbereiteten Repository-Server initialisieren oder migrieren.

1. Führen Sie das Toolkit im GUI-Modus aus:

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

   Alternativ können Sie das Toolkit auch im Konsolenmodus ausführen:

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

2. Geben Sie den Repository-Pfad an (z. B. in Form einer Position auf dem Hostdateisystem, des Netzes oder einer HTTP-Adresse), wenn das Installationsrepository nicht konfiguriert ist.
3. Wählen Sie IBM SPSS Collaboration and Deployment Services als Paket aus, das installiert werden soll. Sie können auch Adapter oder Komponenten auswählen, die mit dem Server installiert werden sollen, wie z. B. den IBM SPSS Collaboration and Deployment Services Scoring Adapter for PMML. Voraussetzung hierfür ist, dass diese Adapter oder Komponenten in den In stallationsrepositorys verfügbar sind.
4. Lesen Sie die Lizenzvereinbarung und akzeptieren Sie deren Bedingungen.

5. Geben Sie die Paketgruppe und das Installationsverzeichnis an. Für diese Installation ist eine neue Paketgruppe erforderlich.
6. Geben Sie das Installationsverzeichnis für gemeinsam genutzte Ressourcen an. Sie können das Verzeichnis für gemeinsam genutzte Ressourcen nur bei der Erstinstallation eines Pakets angeben.
7. Wählen Sie **Vorbereitung für Docker** als Bereitstellungsziel aus.
8. Geben Sie Informationen zur Datenbankverbindungsinformationen an:
   - **Datenbanktyp.** IBM DB2, SQL Server oder Oracle.
   - **Host.** Der Hostname oder die Adresse des Datenbankservers.
   - **Port.** Der Zugriffsport für den Datenbankserver.
   - **Datenbankname.** Der Name der Datenbank, die für das Repository verwendet werden soll.
   - **Quellen-ID/Servicename.** Bei Oracle die Quellen-ID oder der Servicename.
   - **Benutzername.** Der Datenbankbenutzername.
   - **Kennwort.** Das Kennwort des Datenbankbenutzers.
   - Geben Sie bei der Wiederverwendung einer Datenbank aus einer vorherigen Installation an, ob vorhandene Daten beibehalten oder verworfen werden sollen.
9. Geben Sie Optionen für den Keystore für Verschlüsselungsschlüssel an. Bei dem Keystore handelt es sich um eine verschlüsselte Datei, die den Schlüssel zum Entschlüsseln der Kennwörter enthält, die vom Repository verwendet werden (z. B. das Kennwort für die Repository-Verwaltung und das Kennwort für den Datenbankzugriff).
   - Geben Sie zur Wiederverwendung eines Keystores aus einer vorhandenen Repository-Installation den Pfad und das Kennwort für den Keystore an. Der Schlüssel aus dem alten Keystore wird extrahiert und im neuen Keystore verwendet. Beachten Sie, dass die JRE, die zur Ausführung des Anwendungsservers verwendet wird, mit der JRE kompatibel sein muss, die zum Erstellen der Verschlüsselungsschlüssel verwendet wurde.
   - Wenn Sie einen vorhandenen Keystore nicht wiederverwenden, geben Sie das Kennwort für den neuen Keystore an und bestätigen Sie dieses. Der Keystore wird unter `<Repository-Installationsverzeichnis>/keystore` erstellt.
10. Geben Sie das Kennwort an, das für das Benutzerkonto des Administrators (admin) für das integrierte Repository verwendet werden soll. Dieses Kennwort wird bei der ersten Anmeldung beim Repository verwendet.
11. Klicken Sie auf **Installieren**.

Ausführen des Toolkits im unbeaufsichtigten Modus

Sie können das Toolkit automatisieren, indem Sie IBM Installation Manager im unbeaufsichtigten Modus mit Eingaben aus einer Antwortdatei von IBM Installation Manager ausführen. Die Vorlage für die Antwortdatei ähnelt den folgenden Angaben:

```
<?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 8.3.0' installLocation='/opt/IBM/
SPSS/Deployment/8.3.0/Server'>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='user.KeyPassUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
    <data key='user.ReuseKeyUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='false'/>
    <data key='user.KeyPwdUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
    <data key='user.AdminPassUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
    <data key='user.AdminPwdUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
    <data key='user.DBPort,com.ibm.spss.cds.server.v8.3.0.offering' value='50000'/>
    <data key='user.DBName,com.ibm.spss.cds.server.v8.3.0.offering' value='cadsdb'/>
    <data key='user.DBHost,com.ibm.spss.cds.server.v8.3.0.offering' value='x.x.x.x'/>
```

```
    <data key='user.DBTypeUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='db2'/>
    <data key='user.DataEraseUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='false'/>
    <data key='user.DBPassword,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
    <data key='user.SSLServiceUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='false'/>
    <data key='user.OracleServiceUserData,com.ibm.spss.cds.server.v8.3.0.offering' value='fal
se'/>
    <data key='user.DBUsername,com.ibm.spss.cds.server.v8.3.0.offering' value='xxxx'/>
  </profile>
  <install>
    <!-- IBM SPSS Collaboration and Deployment Services - Repository Server 8.3.0.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.3.0'
id='com.ibm.spss.cds.server.v8.3.0.offering' features='deploy.docker'/>
    <!-- IBM SPSS Modeler Adapters for Collaboration and Deployment Services 18.3.0.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.3.0'
id='com.ibm.spss.modeler.adapter.18.3.0' features='main.feature,text.analytics'/>
    <!-- IBM SPSS PMML Scoring Adapter 8.3.0.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.3.0'
id='com.ibm.spss.pmml.scoring.adapter.v8.3.0' features='main.feature'/>
  </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 -ac
ceptLicense -showProgress
```

Wichtig: Erstellen Sie eine Sicherungskopie der Keystore-Datei. Wenn Sie die Keystore-Datei verlieren, ist der Repository-Server nicht in der Lage, Kennwörter zu entschlüsseln, und kann nicht mehr verwendet werden. Dies macht eine Neuinstallation erforderlich.

Weitere Hinweise zur Migration

Bei der IBM SPSS Collaboration and Deployment Services Repository-Migration bleiben die Inhalte und Konfigurationseinstellungen eines vorhandenen Repositorys erhalten.

Bei dem für Docker vorbereiteten Repository wird das folgende Migrationsszenario unterstützt.

- Migration von einer früheren Version der Repository-Datenbank. Für IBM SPSS Collaboration and Deployment Services 8.3.0 wird eine Migration von Version 8.2.2 unterstützt.
- Migration von einem anderen Host, Anwendungsserver oder Datenbankserver. Der für Docker vorbereitete IBM SPSS Collaboration and Deployment Services Repository-Server kann eine Verbindung zu einer vorhandenen Repository-Datenbank der Version 8.3.0 herstellen.

Wichtig: Aufgrund der Verwendung eines Keystores muss die JRE vor und nach der Migration mit der IBM JRE identisch sein.

Hinweise

- Bei der Einstellung `url_prefix` handelt es sich um die URL für die Weiterleitung der vom Server initiierten Anforderungen. Der Präfixwert muss extern auflösbar sein, wenn externe Clients eine Verbindung zum Repository herstellen. Aufgrund des komplexen Konfigurationsszenarios von Docker-Netzwerken muss diese Einstellung manchmal manuell konfiguriert werden.
  - Legen Sie bei einer einzelnen Containerinstanz des Repositorys `url_prefix` auf den Namen des Hosts des Docker-Dämons und auf den Port fest, der vom Container bereitgestellt wird.
  - Legen sie bei Clustering-Containerinstanzen (Swam, Kubernetes, etc.) `url_prefix` auf die Adresse des Reverse-Proxy-Servers (z. B. Ngnix) fest.
- Auf dem für Docker vorbereiteten Repository-Server der Version 8.3.0 wurde bereits der Modeler Adapter der Version 18.3.0 installiert und konfiguriert. Für den Adapter ist keine zusätzliche Konfiguration erforderlich.
- Die Zeitzone der einzelnen Container kann vom Docker-Dämon abweichen. Dies ist eine Einschränkung von Docker selbst. Sie können die Zeitzoneneinstellungen aktualisieren, indem Sie `docker run` in der

Datei `cdsServer.bat/cdsServer.sh` manuell ändern. Beispiel: `docker run -e TZ=Europe/Amsterdam`

- Bekannte Probleme:
  - Im Clustering-Modus kann die Scoring-Konfiguration zwischen den Containern ggf. nicht ordnungsgemäß synchronisiert werden. Sollte dieses Problem auftreten, starten Sie den Container erneut. Die Synchronisierung sollte dann beim Start aufgerufen werden.
  - SSL ist standardmäßig nicht aktiviert. Für die Verwendung von SSL müssen Sie ggf. das SSL-Zertifikat ggf. manuell in den Container importieren und konfigurieren.

Deinstallieren

Für den Fall, dass eine Installation nicht mehr 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, nehmen Sie die Bereitstellung der Repository-Ressourcen auf dem Anwendungsserver zurück:
   - WebSphere-Standalone-Server

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

   - Von 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. Wenn Sie alle Daten in der Repository-Datenbank löschen möchten, öffnen Sie die Konfigurationsdatei *<Repository-Installationsverzeichnis>/uninstall/uninstall.properties* und legen Sie die Eigenschaft `cds.uninstall.remove.user.data property` auf `true` fest. Beachten Sie, dass einige Daten nach der Deinstallation von IBM Installation Manager in der Datenbank verbleiben und manuell gelöscht werden müssen.

   Wichtig: Führen Sie diesen Schritt nicht aus, wenn Sie das Repository erneut für neue Installationen verwenden möchten oder die Audit- oder Protokollierungsdaten beibehalten müssen. Zudem sollten Sie in Erwägung ziehen, mithilfe der Tools des Datenbankanbieters eine Datenbanksicherung zu erstellen, bevor Sie diese Option verwenden.
4. Führen Sie IBM Installation Manager (GUI oder Befehlszeile) aus, wählen Sie die Option zum Deinstallieren von IBM SPSS Collaboration and Deployment Services aus und befolgen Sie die Eingabeaufforderungen. IBM Installation Manager kann auch im unbeaufsichtigten Modus ausgeführt werden. Weitere Informationen finden Sie in der Dokumentation zu IBM Installation Manager: http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.
5. Löschen Sie manuell das Stamminstallationsverzeichnis für das Repository.

   Wichtig: Wenn Sie Repository-Daten wiederverwenden möchten, wird empfohlen, die Keystore-Datei zu speichern, die sich unter *<Repository-Installationsverzeichnis>/keystore* befindet.

Kapitel 3. Migration

Bei der IBM SPSS Collaboration and Deployment Services Repository-Migration bleiben die Inhalte und Konfigurationseinstellungen eines vorhandenen Repositorys enthalten. Dazu zählen:

- Repository-Dateien und Ordnerstruktur
- Zeitplanungs- und Benachrichtigungskomponenten
- Benachrichtigungsvorlagen
- Lokale Benutzer
- Lokal definierte Überschreibungen von Benutzerlisten und Gruppen des fernen Verzeichnisses
- Rollendefinitionen und Zugehörigkeit
- Benutzervorgaben
- Symbole

Folgende Migrationsszenarien werden unterstützt:

- Migration von einer früheren Version des Repositorys.
- Migration zu einem anderen Host, Anwendungsserver oder Datenbankserver.

Folgende Pfade können für die Migration verwendet werden:

- Installation mit einer Kopie der Repository-Datenbank. Diese Methode wird für die Migration empfohlen.
- Installation des Repositorys mit einer vorhandenen Repository-Datenbank.

Bevor Sie einen Migrationspfad auswählen, sollten Sie dieses gesamte Kapitel lesen, einschließlich der Informationen zu zusätzlichen Hinweisen zur Migration.

Unabhängig vom ausgewählten Migrationspfad müssen Sie folgende Richtlinien befolgen:

- IBM SPSS Collaboration and Deployment Services Repository-Anwendungsdateien müssen an einer anderen Position als bei der ursprünglichen Installation installiert werden. Überschreiben Sie nicht die Dateien an der ursprünglichen Position.
- Es muss eine neue Anwendungsserverinstanz erstellt werden. Verwenden Sie das Profil (WebSphere) bzw. den Server (JBoss) nicht wieder, das bzw. der bereits verwendet wird, um die alte Instanz des Repositorys auszuführen.
- Beim Migrationsprozess wird die Konfiguration des Repository-Pakets nicht beibehalten, sodass sämtliche zusätzliche Pakete für IBM SPSS-Produkte wie IBM SPSS Modeler und IBM SPSS Statistics erneut installiert werden müssen. Die Pakete in der Zielinstanz müssen sich auf derselben oder einer höheren Ebene befinden wie die Pakete im Quellenrepository. Sie sollten hierzu auf die Datenbanktabelle verweisen. Die Pakete müssen sich auf einer Ebene befinden, die mit der angegebenen Zielversion von IBM SPSS Collaboration and Deployment Services kompatibel ist. Weitere Informationen finden Sie im Thema „ IBM SPSS-Produktkompatibilität” auf Seite 30.

  Anmerkung: Die Pakete in der Zielinstanz müssen sich auf derselben Versionsebene oder einer höheren Ebene befinden wie die Pakete in der Quelleninstanz. Die Informationen zu installierten Paketen und den zugehörigen Versionen können in der Tabelle SPSSSETUP_PLUGINS der Datenbank der Quelleninstanz gefunden werden.

Installation mit einer Kopie der Repository-Datenbank

Durch die Verwendung einer Kopie einer vorhandenen Repository-Datenbank kann die vorhandene Instanz so lange online bleiben, bis die neue Installation in Betrieb genommen werden kann.

Diese Prozedur dient der Migration mit einer Kopie der Repository-Datenbank, wobei die Quellen- und die Zieldatenbank identisch sind (z. B. von Db2 zu Db2). Informationen zum Wechseln von Datenbanksystemen finden Sie unter „Migration in eine andere Datenbank” auf Seite 38

- Erstellen Sie eine Kopie der vorhandenen Repository-Datenbank. Die Datenbankkopie kann mithilfe des Datenbankanbieters oder mithilfe von Tools von anderen Anbietern durchgeführt werden.
- Führen Sie das Konfigurationsdienstprogramm von IBM SPSS Collaboration and Deployment Services aus und verweisen Sie es auf die neue Kopie der Repository-Datenbank. Stellen Sie sicher, dass die Option "Vorhandene Daten beibehalten" ausgewählt ist, damit alle vorhandenen Daten beibehalten werden.
- Installieren Sie zusätzliche Pakete erneut.

Installation mit einer vorhandenen Repository-Datenbank

Sie können auch ein Upgrade auf IBM SPSS Collaboration and Deployment Services Repository durchführen, indem Sie das System mit einer vorhandenen Repository-Datenbank installieren.

- Stoppen Sie das Repository.
- Sichern Sie die vorhandene Repository-Datenbank.
- Installieren Sie IBM SPSS Collaboration and Deployment Services und führen Sie das Konfigurationsdienstprogramm aus. Stellen Sie sicher, dass die Option "Vorhandene Daten beibehalten" ausgewählt ist, damit alle vorhandenen Daten beibehalten werden.
- Installieren Sie zusätzliche Pakete erneut.

Migration in eine andere Datenbank

Die Migration in eine andere Datenbank kann den Wechsel zu einem anderen Datenbankanbieter (z. B. von SQL Server zu IBM Db2 oder von Oracle zu Db2) oder die Migration in eine Datenbank auf einem anderen Betriebssystem (z. B. von Db2 for i zu Db2 für Linux, UNIX und Windows) beinhaltn.

Repository-Objekte können in die Datenbank eines anderen Anbieters übertragen werden, indem in der neuen Datenbank eine Kopie der alten Datenbank erstellt wird.

- Erstellen Sie die Zieldatenbank nach den Anweisungen, die mit dem Release von IBM SPSS Collaboration and Deployment Services bereitgestellt werden, über das Sie die Migration durchführen.
- Verwenden Sie die Tools des Datenbankanbieters, um die Daten aus der Datenbank des Quellenrepositorys in die Datenbank des Zielrepositorys zu verschieben. Die Datenbank müsste bereits konfiguriert sein. Daher müssen die Daten lediglich in die IBM SPSS Collaboration and Deployment Services-Tabellen verschoben werden. Weitere Informationen finden Sie in der Dokumentation des Datenbankanbieters.
- Erstellen Sie eine Kopie der Keystore-Datei, die von der Datenbank des Quellenrepositorys 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 "Vorhandene Daten beibehalten" ausgewählt ist, damit alle vorhandenen Daten beibehalten werden.
  - Wählen Sie bei entsprechender Aufforderung für den Keystore die Kopie der Keystore-Datei aus, die für die neue Instanz verwendet werden soll.
- Installieren Sie zusätzliche Pakete erneut.

Beachten Sie, dass Sie aufgrund von Unterschieden zwischen Datenbankumgebungen und Tools des Anbieters zum Kopieren (z. B. Db2-Backup, MS-SQL Server-Backup oder Oracle RMAN) während der Migration prüfen müssen, ob folgende Datenbankfunktionen von dem Tool unterstützt werden, das Sie ausgewählt haben:

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

Oracle 12cR1 Data Pump unterstützt beispielsweise keine XML-Tabellen. Es kann daher für die Wiederherstellung sämtlicher Repository-Tabellen verwendet werden, mit Ausnahme der beiden XML-Tabellen. Die XML-Tabellen können mit Oracle Export migriert werden. Prüfen Sie alle Anforderungen an den Datenbankanbieter, wie z. B. die Registrierung des XML-Schemas auf dem MS SQL Server und in Oracle. Es wird empfohlen, sich vor der Migration der Datenbank von dem Datenbankadministrator beraten zu lassen.

Fehler bei der Migration von Daten von 12c zu 19c

Beachten Sie beim Upgrade von 12c auf 19c, dass folgende neun Benutzerrollennamen aus 12c in 19c nicht mehr vorhanden sind:

- XS_RESOURCE
- JAVA_DEPLOY
- SPATIAL_WFS_ADMIN
- WFS_USR_ROLE
- SPATIAL_CSW_ADMIN
- CSW_USR_ROLE
- APEX_ADMINISTRATOR_ROLE
- APEX_GRANTS_FOR_NEW_USERS_ROLE
- DELETE_CATALOG_ROLE

Wenn Sie diese Rollen in 12c verwendet haben, werden Ihnen beim Importieren von Daten in 19c folgende Fehler angezeigt:

```
ORA-39083: Object type ROLE_GRANT failed to create with error:
ORA-01919: role 'XXX' does not exist
Failing sql is:
 GRANT "XXX" TO "%schemaName%" WITH ADMIN OPTION
```

Da sich einige Rollennamen in 19c geändert haben, sollte Ihr Datenbankadministrator sicherstellen, dass vor dem Import entsprechende neue Rollenberechtigungen manuell erteilt werden. Auf diese Weise wird verhindert, dass diese Fehler die Installation und Verwendung von IBM SPSS Collaboration and Deployment Services beeinträchtigen.

Weitere Hinweise zur Migration

Je nach Konfiguration sind ggf. zusätzliche Aufgaben erforderlich, damit folgende Komponenten erfolgreich migriert werden:

- Kennwörter
- JMS-Datenspeicher
- Benachrichtigungsvorlagen

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

Migrieren von Kennwörtern

Es empfiehlt sich, bei der Migration auf eine neue IBM SPSS Collaboration and Deployment Services-Instanz als ursprüngliche Installation eine Java-Umgebung desselben Anbieters mit derselben Bitgröße (32-Bit oder 64-Bit) zu verwenden. Grund hierfür ist, dass die Kennwörter, die im Repository gespeichert sind, basierend auf einem Keystoreschlüssel verschlüsselt wurden, der von der Java Runtime bereitgestellt wird. Eine andere Java-Bitgröße oder eine andere anbieterspezifische Implementierung weist einen anderen Keystoreschlüssel auf, mit dem die Kennwörter nicht korrekt entschlüsselt werden können. In einigen Fällen müssen Java-Anbieter und -Bitgröße geändert werden (z. B. beim Wechsel von JBoss zu WebSphere).

Wenn sich die Java-Verschlüsselung, die bei der Installation des Repositorys über eine vorhandene Datenbank verwendet wird, von der Verschlüsselung unterscheidet, die von der ursprünglichen Instanz verwendet wird (z. B. IBM Java-Verschlüsselung vs. Sun Java-Verschlüsselung), werden die Berechtigungsnachweiskennwörter nicht migriert. Ferner meldet das Konfigurationsdienstprogramm einen Fehler. Das Repository kann jedoch trotzdem gestartet werden. Und Sie können Berechtigungsnachweiskennwörter manuell mithilfe von IBM SPSS Deployment Manager ändern. Das Export-/Importdienstprogramm migriert zwar Kennwörter, bei der Wiederverwendung einer vorhandenen Datenbank muss der Export jedoch über die Quelleninstallation durchgeführt werden, bevor die Ressourcen der Berechtigungsnachweise in die Zielinstallation importiert werden.

Wenn Sie eine andere Java-Umgebung verwenden müssen, können Sie die Kennwörter in den Ressourcendefinitionen der Berechtigungsnachweise und IBM SPSS Modeler-Jobschritten nach der Konfiguration des IBM SPSS Collaboration and Deployment Services Repositorys ersetzen:

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

oder

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

Migration des JMS-Speichers in WebSphere

Wenn das IBM SPSS Collaboration and Deployment Services Repository mit einem WebSphere Application Server installiert wird, wird der WebSphere JMS-Standardprovider, Service Integration Bus (SIB), so konfiguriert, dass die Repository-Datenbank als JMS-Nachrichtenspeicher verwendet wird. 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.

Bei Verwendung einer Datenbankkopie zum Migrieren der Inhalte eines Repositorys zu einer neuen Instanz, die in 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.

Wenn Sie unter z/OS mit Db2 WebSphere-JMS-Nachrichtenspeichertabellen manuell erstellen möchten, können Sie mit dem WebSphere-Befehl *sibDDLGenerator* die DDL generieren und die DDL anschließend auf die Datenbank anwenden, um die Tabellen zu erstellen. Weitere Informationen zu *sibDDLGenerator* finden Sie in der WebSphere-Dokumentation.

Migration von Benachrichtigungsvorlagen

Damit die an den Benachrichtigungsvorlagen vorgenommenen Anpassungen in einem vorhandenen Repository beibehalten werden, müssen Sie die Vorlagen aus *<Repository-Installationsverzeichnis>/components/notification/templates* in dasselbe Verzeichnis der neuen Installation kopieren, nachdem die neue Installation anfänglich konfiguriert wurde. Weitere Informationen zu Benachrichtigungsvorlagen finden Sie im *Administratorhandbuch zu IBM SPSS Collaboration and Deployment Services Repository 8.3.0*.

Kapitel 4. Paketmanagement

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

Details finden Sie in den Installationsanweisungen für einzelne Komponenten.

Sie können auch das IBM SPSS Collaboration and Deployment Services Package Manager-Dienstprogramm verwenden, um Fehler bei der IBM SPSS Collaboration and Deployment Services-Paketkonfiguration zu beheben und zusätzliche Komponenten zu installieren, wie z. B. benutzerdefinierte Inhaltsadapter und Sicherheitsprovider.

Installieren von Paketen

IBM SPSS Collaboration and Deployment Services Package Manager ist eine Befehlszeilenanwendung. Es kann auch von anderen Anwendungen im Stapelmodus aufgerufen werden, damit diese im Repository ihre Paketdateien installieren können.

Wenn das IBM SPSS Collaboration and Deployment Services Repository anfänglich automatisch bereitgestellt wurde, muss der Anwendungsserver bei der Paketinstallation folgenden Status aufweisen:

- JBoss: Gestoppt
- Liberty: Gestoppt

Der Benutzer muss über Berechtigungen auf Administratorebene verfügen, um Pakete installieren zu können.

Der Paketmanager führt eine Versionsprüfung durch, um zu verhindern, dass die neuere Version eines Pakets durch eine ältere Version überschrieben wird. Der Paketmanager prüft zudem erforderliche Komponenten, um sicherzustellen, dass diese installiert wurden und ihre Versionen der erforderlichen Version oder einer neueren Version entsprechen. Die Prüfungen können überschrieben werden, beispielsweise um eine ältere Version des Pakets zu installieren.

Anmerkung: Abhängigkeitsprüfungen können nicht überschrieben werden, wenn der Paketmanager im Stapelmodus aufgerufen wird.

So installieren Sie ein Paket

1. Navigieren Sie zu *<Repository-Installationsverzeichnis>/bin/*.
2. Führen Sie je nach Betriebssystem *cliPackageManager.bat* unter Windows oder *cliPackageManager.sh* unter UNIX aus.
3. Geben Sie bei entsprechender Aufforderung den Benutzernamen und das 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 im folgenden Beispiel dargestellt:

   ```
   install 'C:\dir one\package1.package'
   ```

   Wenn Sie mehrere Pakete gleichzeitig installieren möchten, geben Sie mehrere Paketnamen getrennt durch ein Leerzeichen ein. Beispiel:

   ```
   install 'C:\dir one\package1.package' 'C:\dir one\package2.package'
   ```

Eine alternative Möglichkeit zur Installation mehrerer Pakete besteht in der Verwendung des Parameters `-dir` oder `-d` mit dem Pfad eines Verzeichnisses, das die zu installierenden Pakete enthält.

```
install -dir 'C:\cds_packages'
```

Bei fehlgeschlagenen Abhängigkeiten oder Versionsprüfungen werden Sie wieder zur anfänglichen Eingabeaufforderung des Paketmanagers geleitet. Führen Sie den Installationsbefehl mit dem Parameter `-ignore` oder `-i` erneut aus, wenn bei der Installation nicht schwerwiegende Fehler ignoriert werden sollen.

5. Verwenden Sie nach Abschluss der Installation den Befehl `exit`, um den Paketmanager zu beenden.

   Geben Sie `help` ein und drücken Sie die `Eingabetaste`, um weitere Installationsoptionen für die Befehlszeile anzuzeigen. Zu den Optionen gehören:

   - `info "<Paketpfad>"`: Anzeige von Informationen für eine bestimmte Paketdatei.
   - `install "<Paketpfad>"`: Installation der angegebenen Paketdateien im Repository.
   - `tree`: Anzeige von Informationen zur Baumstruktur des installierten Pakets.

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> [<weiterer_Paketpfad>]
```

Protokollierung

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

Kapitel 5. 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 das browserbasierte IBM SPSS Deployment Manager nicht zulässig.

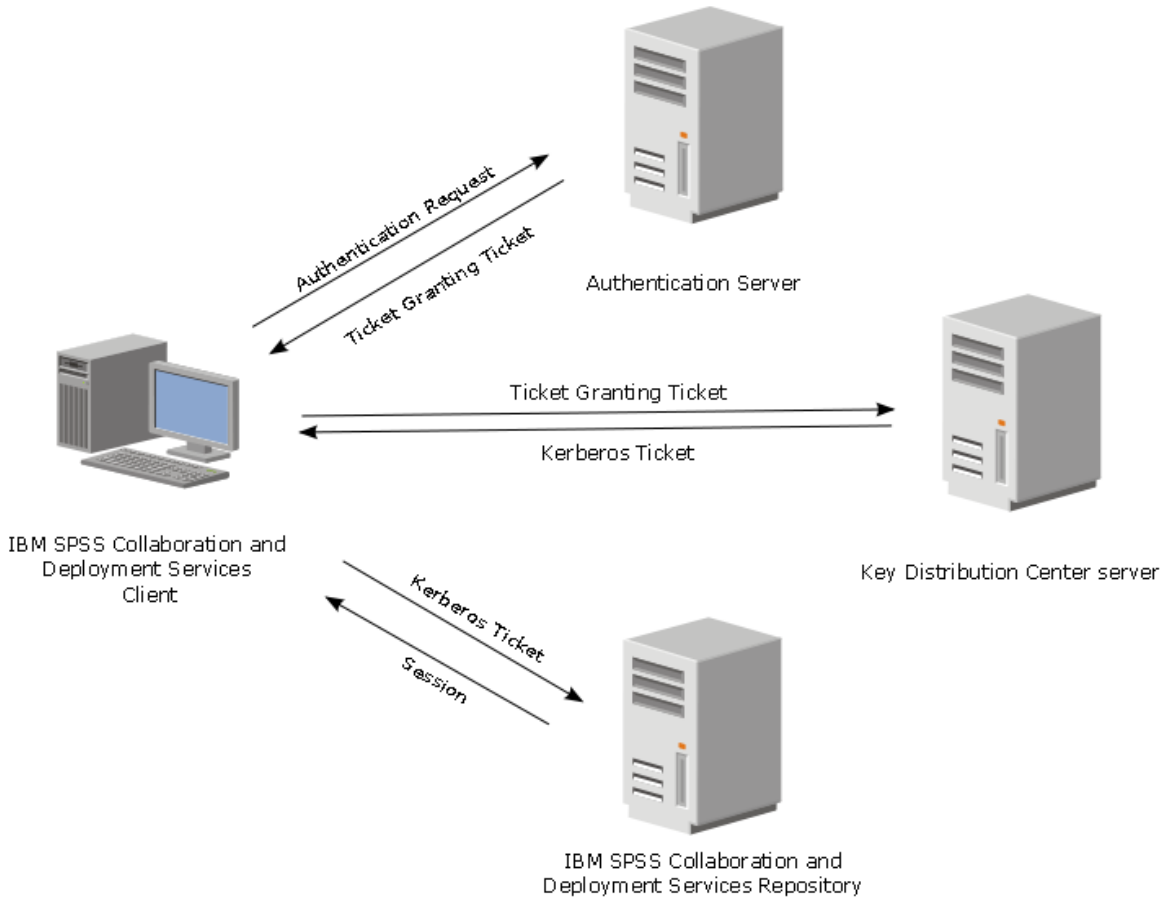

Abbildung 3. IBM SPSS Collaboration and Deployment Services-SSO-Architektur

Wenn IBM SPSS Collaboration and Deployment Services beispielsweise in Verbindung mit Windows Active Directory verwendet wird, müssen Sie den KDC-Dienst (KDC = *Kerberos Key Distribution Center*) konfigurieren, um Single Sign-on zu aktivieren. Der Dienst stellt für Benutzer und Computer Sitzungstickets und vorübergehende Sitzungsschlüssel in einer Active Directory-Domäne bereit. Der KDC muss im Rahmen der Active Directory Domain Services (AD DS) auf den einzelnen Domänencontrollern ausgeführt werden. Wenn Single Sign-on aktiviert ist, melden sich IBM SPSS Collaboration and Deployment Services-Anwendungen bei einer Kerberos-Domäne an und verwenden Kerberos-Token für die Web-Service-Authentifizierung. Wenn Single Sign-on aktiviert ist, wird dringend empfohlen, die SSL-Kommunikation für das Repository zu konfigurieren.

Desktop-Clientanwendungen wie Deployment Manager erstellen ein Java-Subjekt und bauen dann über diesen Kontext mit dem Repository eine GSS-Sitzung auf. Das Repository gibt ein Kerberos-Service-Ticket an den Client zurück, wenn der GSS-Kontext erstellt wurde. Thin-Client-Anwendungen wie Deployment Portal erhalten ebenfalls ein Kerberos-Service-Ticket aus dem Repository. Thin Clients führen jedoch zu-

nächst eine HTTP-basierte, plattformübergreifende Authentifizierung über das Negotiate-Protokoll durch. Sowohl bei Desktop- als auch bei Thin-Client-Anwendungen müssen Sie sich zunächst bei einer Kerberos-Domäne anmelden, z. B. bei Ihrer Microsoft Active Directory-/Windows-Domäne.

Die Single-Sign-on-Konfiguration 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* über die Registerkarte "Serveradministration" von IBM SPSS Deployment Manager. Weitere Informationen finden Sie in der Administratordokumentation zu IBM SPSS Collaboration and Deployment Services.
- Konfiguration des Kerberos Key Distribution Center-Servers. Auf dem Kerberos Key Distribution Center-Server muss die Übertragung von Berechtigungsnachweisen für den Kerberos-Service-Prinzipal aktiviert sein. Die Prozedur zur Aktivierung der Übertragung von Berechtigungsnachweisen variiert je nach Verzeichnisserver und Kerberos-Umgebung.
- Konfiguration des Kerberos Key Distribution Center-Servers als IBM SPSS Collaboration and Deployment Services-Single-Sign-on-Provider über die 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 LSA-Zugriff auf den Kerberos-Server aktualisiert werden.
- Abhängig von dem Anwendungsserver, der mit dem Repository verwendet wird, muss die Anwendungsserverkonfiguration ggf. aktualisiert werden.
- Bei Windows-Clientsystemen muss der Registrierungswert `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\` aktualisiert werden. Weitere Informationen finden Sie im Thema „Aktualisierung der Windows-Registrierung für Single Sign-on” auf Seite 49.
- Für den Thin-Client-Zugriff auf das Repository (z. B. mit IBM SPSS Collaboration and Deployment Services Deployment Portal) muss auf dem Web-Browser SPNEGO (Simple and Protected GSS-API Negotiation) aktiviert sein.

Zudem sind für die Aktivierung des Berechtigungsnachweises für die Serverprozesse für das Repository weitere Konfigurationsschritte erforderlich. Weitere Informationen finden Sie im Thema „Konfiguration des Berechtigungsnachweises für Serverprozesse” auf Seite 50.

Verzeichniskonfiguration für Single Sign-on

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

- OpenLDAP-Verzeichnis
- Microsoft Active Directory

OpenLDAP

Die Gesamtkonfiguration umfasst die folgenden Schritte:

- Konfigurieren des OpenLDAP-Sicherheitsproviders. Weitere Informationen finden Sie im *Administratorhandbuch zu IBM SPSS Collaboration and Deployment Services 8.3.0*.
- Für den Kerberos-Server spezifische Änderungen an der OpenLDAP-Konfiguration abhängig von dem verwendeten Kerberos-Server.

OpenLDAP mit dem Windows-Kerberos-Server

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

MIT-Kerberos-Server

Wenn der MIT-Kerberos-Server mit OpenLDAP verwendet wird, muss SSL möglicherweise auf dem OpenLDAP-Server und -Client eingerichtet werden, damit eine sichere Kommunikation gewährleistet ist, wenn sich der KDC-Dienst und der LDAP-Server auf einem anderen Host befinden. Aktualisierte Informationen finden Sie in der releasebezogenen Dokumentation zum MIT-Kerberos-Server.

Active Directory

Folgende Anweisungen gelten für den Windows Server 2003-Domänencontroller. Die Schritte sind mit denen für Windows Server 2012-Systeme vergleichbar.

1. Erstellen Sie ein Benutzerprofil, das als Kerberos-Service-Prinzipal verwendet wird.
2. Ordnen Sie dieses Benutzerprofil dem IBM SPSS Collaboration and Deployment Services-Hostsystem zu.
3. Konfigurieren Sie den Verschlüsselungstyp und die Übertragung von Kerberos-Berechtigungsnachweisen.
4. Erstellen Sie eine Kerberos-Chiffrierschlüsseldatei und speichern Sie diese auf dem IBM SPSS Collaboration and Deployment Services-Hostsystem

Nachdem Sie diese Schritte ausgeführt haben, können Sie mithilfe von Deployment Manager Active Directory als Sicherheitsprovider und anschließend einen Kerberos-Single-Sign-on-Provider konfigurieren.

So erstellen Sie ein Benutzerprofil für den Kerberos-Prinzipal

1. Erstellen Sie über die Active Directory-Benutzer und die Computerverwaltungskonsole einen Domänenbenutzer für die ausgewählte Domäne (z. B. Benutzer `krb5.principal` in der Domäne `spss`). Dieser Benutzer entspricht dem Kerberos-Service-Prinzipal.
2. Geben Sie einen Nachnamensparameter für diesen Benutzer an. Dieser ist für einige Anwendungsserver erforderlich.
3. Wählen Sie die Option aus, dass das Kennwort niemals ablaufen soll.

So ordnen Sie dem IBM SPSS Collaboration and Deployment Services-Hostsystem das Benutzerprofil zu

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

Das Tool **`setspn`** greift auf die SPN-Eigenschaft eines Benutzers zu, aktualisiert und entfernt diese. Verwenden Sie folgende Befehlssyntax, um einen SPN hinzuzufügen:

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

Mit der Option `-A` wird dem Domänenkonto ein beliebiger SPN hinzugefügt. Die anderen Argumente weisen folgende Definitionen auf:

<SPN>
Der SPN, der dem Benutzer hinzugefügt wird und das Format *<Serviceklasse>/<Host>* aufweist. Der Wert *<Serviceklasse>* bezeichnet die Klasse des Service. Der Wert *<Host>* entspricht dem Hostnamen, der vollständig qualifiziert oder vereinfacht ist.

<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 vereinfachten, gekürzten Hostnamen hinzu, da ein Client auf beide Namen verweisen könnte.

1. Wenn Sie nicht über das Tool **setspn** verfügen, laden Sie eine entsprechende Version der Windows-Supportools herunter und installieren Sie diese.
2. Führen Sie **setspn** mit dem vollständig qualifizierten Hostnamen des IBM SPSS Collaboration and Deployment Services-Servers als Argument aus, wie im folgenden Beispiel dargestellt:

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

3. Führen Sie **setspn** mit dem Hostnamen des IBM SPSS Collaboration and Deployment Services-Servers als Argument aus, wie im folgenden Beispiel dargestellt:

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

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

So konfigurieren Sie den Verschlüsselungstyp und die Übertragung von Berechtigungsnachweisen

1. Wählen Sie im Dialogfeld "Benutzereigenschaften" auf der Registerkarte "Konto" die Option zur Verwendung der AES-Verschlüsselung aus.
2. Wählen Sie im Dialogfeld "Benutzereigenschaften" auf der Registerkarte "Übertragung" die Option aus, mit der der Benutzer eine Übertragung an einen beliebigen Service vornehmen kann.

So erstellen Sie eine Kerberos-Chiffrierschlüsseldatei

Eine Chiffrierschlüsseldatei enthält Kerberos-Prinzipale mit den entsprechenden verschlüsselten Schlüsseln. Sie wird für die Prinzipalauthentifizierung verwendet. Verwenden Sie für die Erstellung einer Chiffrierschlüsseldatei das Tool **ktpass**. Weitere Informationen zu dem Tool **ktpass** finden Sie unter http://technet.microsoft.com/en-us/library/cc753771.aspx.

1. Führen Sie das Tool **ktpass** wie in dem 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_Serviceproviders>@<Domäne>*.
   - Der Wert für die Option **mapUser** muss folgendes Format aufweisen: *<Kerberos-Service-Prinzipal>@<Domäne>*.
   - Jede Form einer starken Verschlüsselung gemäß der Definition durch die Option **crypto** erfordert die JCE-Erweiterung für eine starke Verschlüsselung von Oracle.
2. Speichern Sie die generierte Chiffrierschlüsseldatei (in diesem Beispiel *c:\temp\krb5.prin.keytab*) auf dem Dateisystem Ihres IBM SPSS Collaboration and Deployment Services-Hosts.

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

Konfiguration des Kerberos-Servers

In der Microsoft Windows-Umgebung wird bei der Verwendung von Active Directory Server mit Windows (integriert) der Kerberos-Server empfohlen. Für den LSA-Zugriff auf den Kerberos-Server müssen Sie die Registry sämtlicher Clientsysteme aktualisieren. Für die Verwendung von Kerberos müssen Sie zudem bestimmte Änderungen an den Browsern vornehmen. Bei Kerberos-Servern, die nicht in einer Microsoft Windows-Umgebung verwendet werden, müssen Sie ggf. sowohl auf der Hostmaschine des Repositorys als auch auf den einzelnen Clientsystemen zusätzliche Software installieren. In allen Fällen muss der Kerberos-Service-Prinzipal festgelegt werden, damit der Berechtigungsnachweis übertragen werden kann. Zudem müssen Sie für die Übertragung von Berechtigungsnachweisen an den einzelnen Clientsystemen bestimmte Änderungen vornehmen.

Konfiguration des Anwendungsservers für Single Sign-on

Abhängig von dem Anwendungsserver, der mit dem Repository verwendet wird, müssen die Anwendungsservereinstellungen ggf. aktualisiert werden.

WebSphere

Die IBM SPSS Collaboration and Deployment Services-Konfiguration 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 auf der Administrationskonsole Folgendes aus:

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

Definieren der JAAS-JGSS-Richtlinie

1. Wählen Sie auf der Administrationskonsole Folgendes aus:

   Sicherheit > **Sichere Verwaltung, Anwendung und Infrastruktur** > **Java Authentication and Authorization Service** > **Anmeldungen bei Anwendung**
2. Definieren Sie die Eigenschaft *JGSSServer*.
3. Definieren Sie unter "Zusätzliche Eigenschaften" für *JGSSServer* die Modulklasse *com.ibm.security.auth.module.Krb5LoginModule* mit der Authentifzierungsstrategie REQUIRED.
4. Definieren Sie für *com.ibm.security.auth.module.Krb5LoginModule* folgende benutzerdefinierte Eigenschaften.

Eigenschaftsname	**Wert**
credsType	Beide
Principal	<Name des Prinzipals>, z. B. *HTTP/cdsserver.spss.com@SPSS.COM*
useDefaultKeytab	true

JBoss

Für den JBoss Application Server muss mindestens eine JAAS-Konfiguration (Java Authentication and Authorization Service) für JGSSServer und CaDSMiddleTier bereitgestellt werden. Die Vorlage für die Anwen-

dungsrichtlinie von Single Sign-on kann im JGSSServer-Element von <JBoss-Installationsverzeichnis>/standalone/configuration/cds_server.xml gefunden werden. Unter Umständen muss der Name des Kerberos-Anmeldemoduls so geändert werden, dass er mit der JRE des Anwendungsservers übereinstimmt.

Es muss mindestens eine JAAS-Konfiguration für JGSSServer mit folgenden Parametern bereitgestellt werden:

- **JGSSServer** (erforderlich)
- **CaDSMiddleTier** (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=<Gebietsname>
 useKeyTab="true"
 principal=<Name>
 keyTab=<Pfad>
 debug=false;
};
```

2. Die optionale KerberosLocalUser-Konfiguration wird verwendet, um den NTLM-Bypass zu ermöglichen. Mit dieser Konfiguration können Benutzer einen Kerberos-Berechtigungsnachweis erstellen, wenn der Client-Browser während der Verhandlungsherausforderung ein NTLM-Token (anstelle eines Kerberos-Tokens) sendet. Beachten Sie, dass auf Windows-Systemen, bei denen sich der Browser auf demselben System befindet und bei denen der IBM SPSS Collaboration and Deployment Services-Server installiert ist, immer ein NTLM-Token gesendet wird. Alle NTLM-Anfragen an IBM SPSS Collaboration and Deployment Services können inaktiviert werden, indem diese Konfiguration aus der zugehörigen JAAS-Konfigurationsdatei ausgelassen 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 bei Datenbankservern 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. Für Sun JRE wird die folgende CaDSMiddleTier-Standardkonfiguration erstellt:

```
CaDSMiddleTier {
 com.sun.security.auth.module.Krb5LoginModule required
 useTicketCache="true"
 renewTGT="true"
 debug="false";
 realm=<Gebietsname>
```

```
  kdc=<KDC-Name>
};
```

5. Es können auch der entsprechende Name für die Anmeldemodulklasse, der Anforderungstyp und andere Optionen angegeben werden, die das Anmeldemodul für die einzelnen JAAS-Konfigurationen benötigt. Die Anmeldemodulklasse muss sich im Klassenpfad befinden. Weitere Informationen finden Sie in der Herstellerdokumentation zu JRE und Anwendungsserver.

Aktualisierung der Windows-Registrierung für Single Sign-on

Damit SSO ordnungsgemäß funktioniert, muss das Ticket-Granting-Ticket (TGT) von Kerberos den Sitzungsschlüssel enthalten. Zur Aufnahme des Schlüssels muss die Windows-Registrierung aktualisiert werden. Weitere Informationen hierzu finden Sie in http://support.microsoft.com/kb/308339.

IBM SPSS Collaboration and Deployment Services-Installationsmedien enthalten Dateien zur Aktualisierung der Registrierung für die Konfiguration von Windows XP SP2-, Windows Vista- und Windows 2003-Systemen für den auf Kerberos basierenden Single Sign-on. Die Dateien befinden sich im Verzeichnis `/Documentation/Utility_Files/Windows/registry` des Dokumentationspakets (heruntergeladen von IBM Passport Advantage). Es handelt sich um folgende Dateien:

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

Verwenden Sie bei Windows Vista und neueren Systemen die Datei `Win2003_Kerberos.reg`.

Die Registrierungsdateien ermöglichen es dem Systemadministrator, Registrierungsänderungen mit einer Push-Operation 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 gebietsübergreifende Authentifizierung konfigurieren, um den Benutzerzugriff zu steuern.

Angenommen beispielsweise, Sie verfügen über zwei Domänen: `AppDomain` und `UserDomain`. Die beiden Domänen verfügen über eine unidirektionale Vertrauensstellung. Dabei wird die Domäne `AppDomain` für die ausgehende Vertrauensstellung und die Domäne `UserDomain` für die eingehende Vertrauensstellung konfiguriert. Sie installieren den IBM SPSS Collaboration and Deployment Services-Server in der Domäne `AppDomain` und IBM SPSS Deployment Manager in der Domäne `UserDomain`.

Für die Konfiguration von IBM SPSS Collaboration and Deployment Services für die unidirektionale Vertrauensstellung müssen Sie sowohl den IBM SPSS Collaboration and Deployment Services-Server als auch IBM SPSS Deployment Manager ändern.

Konfigurieren des IBM SPSS Collaboration and Deployment Services-Servers

1. Beenden Sie den IBM SPSS Collaboration and Deployment Services-Server.
2. Erstellen Sie auf dem Serverdateisystem die gültige Kerberos-Konfigurationsdatei `krb5.conf`. Die Datei müsste Inhalte ähnlich der folgenden Zeilen aufweisen, wobei die Domänen durch Werte ersetzt werden, die Ihrem System entsprechen:

```
[libdefaults]
default_realm = APPDOMAIN.COM

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

3. Legen Sie die Java-Systemeigenschaft `java.security.krb5.conf` auf die Position der Datei `krb5.conf` fest. Beispiel:

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

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

Konfigurieren von IBM SPSS Deployment Manager

1. Schließen Sie IBM SPSS Deployment Manager.
2. Erstellen Sie im Ordner für die Windows-Installation die gültige Kerberos-Konfigurationsdatei `krb5.ini`, z. B. `c:\windows\krb5.ini`. Die Datei müsste Inhalte aufweisen, die für die gebietsübergreifende Authentifizierung gültig sind, und den folgenden Zeilen ähneln. Dabei werden die Domänen durch Werte ersetzt, die Ihrem System entsprechen:

```
[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 des Berechtigungsnachweises für Serverprozesse

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 Serverprozesse finden Sie in der Dokumentation zu IBM SPSS Deployment Manager.

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

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

So verwenden Sie den Berechtigungsnachweis für Serverprozesse mit Berichtsjobschritten:

- Fügen Sie den Datenbankserver der Datenquelle zur Domäne/zum Gebiet hinzu.
- Konfigurieren Sie den Datenbankserver der Datenquelle so, dass Single-Sign-on-Verbindungen von der Domäne/dem Gebiet akzeptiert werden.
- Konfigurieren Sie die Datenbank der Datenquelle so, dass die entsprechenden Berechtigungen für den Berechtigungsnachweis für Serverprozesse bereitgestellt werden.

So konfigurieren Sie die Benutzeranmeldung der mittleren Ebene in WebSphere

1. Öffnen Sie über die Administrationskonsole

   Sicherheit > **Globale Sicherheit** > **JAAS - Anmeldungen bei Anwendung**
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 für *com.ibm.security.auth.module.Krb5LoginModule* folgende benutzerdefinierte Eigenschaften:
   - useDefaultCache true
   - renewTGT true
   - debug false

So konfigurieren Sie die Benutzeranmeldung der mittleren Ebene in JBoss

Fügen Sie unter *<JBoss-Installationsverzeichnis>/server/<Servername>/conf/login-config.xml* folgende Anwendungsrichtlinie 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>
```

So erstellen Sie den Kerberos-Ticket-Cache

Der Kerberos-Ticket-Cache wird zum Speichern des Kerberos-Tickets verwendet, mit dem der Berechtigungsnachweis für Serverprozesse authentifiziert wird. Führen Sie die folgenden Schritte aus, um den Ticket-Cache zu erstellen:

1. Aktualisieren Sie die Kerberos-Konfigurationsdatei auf dem Host-Server des Repositorys, z. B. *c:\windows\krb5.ini*. Diese Datei gibt das Standardgebiet bzw. die Standarddomäne, Standardcodierungstypen, das erneuerbare Ticket und die KDC-Adresse an und wird von der Anwendung **kinit** zum Generieren unseres Ticket-Cache verwendet. Im Folgenden finden Sie ein Beispiel für die 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 mit den Domänenberechtigungsnachweisen, die für den Berechtigungsnachweis für Serverprozesse verwendet werden, bei dem Repository-Host an. Stellen Sie sicher, dass für diese Berechtigungsnachweise entsprechende Berechtigungen auf dem Host vorliegen.
3. Führen Sie **kinit** über das Verzeichnis der JRE aus, die von dem Repository-Anwendungsserver mit den Optionen zum Erstellen eines erneuerbaren Tickets und eines Ticket-Cache verwendet wird.

   Anmerkung: Unter dem Betriebssystem Windows kann **kinit** kein erneuerbares Ticket erstellen. Fügen Sie folgende Registrierungseinstellung hinzu, um dieses Problem zu beheben:

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

Weitere Informationen finden Sie in der Kerberos-Dokumentation für Ihr Betriebssystem.

4. Geben Sie für den Berechtigungsnachweis für Serverprozesse das Kennwort des Benutzers 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 über die Konfiguration 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. Rufen Sie die *about:config*-URL (Konfigurationsdateieditor von Firefox) auf.
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 Zulassungsliste angeben:

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

Als Mitglied der Zulassungsliste 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

Auch wenn es nicht erforderlich ist, könnten Sie das Tool **kinit.exe** Ihres JDK verwenden, um Ticket-Granting-Tickets von Kerberos abzurufen und zwischenzuspeichern. So können Sie beispielsweise über das Verzeichnis `jre\bin` Ihrer IBM SPSS Deployment Manager-Installation folgenden Befehl ausgeben:

```
kinit.exe -f
```

Mit der Option `-f` wird ein weiterleitbares Ticket erstellt. Mit diesem Befehl wird im Windows-Verzeichnis `Benutzer` eine Cachedatei erstellt, in der die JVM automatisch nach einem Cache sucht.

Wenn Sie diesen Befehl mit einem IBM JDK 7 ausgegeben haben, das älter als 170_SR8 ist, müssen Sie die Datei `krb5.ini` ggf. ändern, um erfolgreich auf diesen Cache zugreifen zu können.

1. Öffnen Sie die Datei `krb5.ini` in einem Texteditor. Die Datei befindet sich häufig im Verzeichnis `C:\Window`.
2. Fügen Sie im Abschnitt **`[libdefaults]:`** folgende Einstellung hinzu:

   ```
   forwardable = true
   ```

3. Speichern Sie die aktualisierte Datei.

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

Kapitel 6. Kontextstammverzeichnisse der Anwendung

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

Eine URL-Referenz auf eine IBM SPSS Collaboration and Deployment Services-Anwendung umfasst folgende Elemente:

URL-Präfix
Umfasst das Protokoll, den Servernamen oder die IP-Adresse und die Portnummer

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

Stammverzeichnis der Anwendung
Gibt das Stammverzeichnis der Anwendung selbst an

Die IBM SPSS Collaboration and Deployment Services Deployment Portal weist beispielsweise 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 Stammverzeichnis des Anwendungsservers. Das Stammverzeichnis der Anwendung lautet `peb`.

Die URL enthält keinen Hinweis dahingehend, dass das Webmodul Teil von IBM SPSS Collaboration and Deployment Services ist. Wenn Sie Ihrem Server andere Anwendungen hinzufügen, erweist sich die Verwaltung der vielen Module, die im Serverstammverzeichnis verfügbar sind, als immer schwieriger.

Wenn Sie den Repository-Server so konfigurieren, dass er als Kontextstammverzeichnis verwendet wird, können Sie die IBM SPSS Collaboration and Deployment Services-Komponenten von anderen Anwendungen isolieren. So können Sie beispielsweise das Kontextstammverzeichnis `ibm/spss` für die IBM SPSS Collaboration and Deployment Services-Module definieren. In diesem Fall lautet die URL für die IBM SPSS Collaboration and Deployment Services Deployment Portal-Schnittstelle wie folgt:

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

Wichtig: Wenn Sie für Ihren Repository-Server ein Kontextstammverzeichnis verwenden, müssen sämtliche Clientanwendungen das gleiche Kontextstammverzeichnis enthalten, wenn sie eine Verbindung zum Server herstellen. Die URL für eine Anwendung, die in der IBM SPSS Collaboration and Deployment Services-Umgebung ausgeführt wird, muss entsprechend aktualisiert werden.

Zugehörige Tasks

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

Aktualisieren von Kontextstammverzeichnissen für WebSphere
Ändern Sie mithilfe der Administrationskonsole die Position, an der auf Anwendungen zugegriffen wird, die in WebSphere bereitgestellt werden.

Aktualisieren von Kontextstammverzeichnissen für JBoss
Ändern Sie die Position, an der auf Anwendungen zugegriffen wird, die in JBoss bereitgestellt werden, indem Sie die EAR-Datei mit den Positionsdefinitionen aktualisieren.

Konfigurieren der Kontextstammverzeichnisse der Anwendung

Für die Konfiguration von Kontextstammverzeichnissen müssen Sie das URL-Präfix des Systems aktualisieren und die einzelnen Spezifikationen der Kontextstammverzeichnisse ändern.

Vorgehensweise

1. Wenn die Verwendung eines URL-Präfix aktiviert ist, fügen Sie dem URL-Präfix das Kontextstammverzeichnis hinzu.
2. Aktualisieren Sie das Kontextstammverzeichnis für jede Anwendung.
   Welche Schritte auszuführen sind, hängt vom Anwendungsserver ab.
   - „Aktualisieren von Kontextstammverzeichnissen für WebSphere” auf Seite 57
   - „Aktualisieren von Kontextstammverzeichnissen für JBoss” auf Seite 57

Ergebnisse

Sie können auf das browserbasierte IBM SPSS Deployment Manager und die IBM SPSS Collaboration and Deployment Services Deployment Portal zugreifen, indem Sie URL-Werte verwenden, die Ihr Kontextstammverzeichnis enthalten.

Nächste Schritte

Aktualisieren Sie alle Verweise auf den Repository-Server, wie z. B. solche, die mit IBM SPSS Deployment Manager definiert wurden, um das Kontextstammverzeichnis in die Server-URL einzuschließen.

Hinzufügen eines Kontextstammverzeichnisses zum URL-Präfix

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

Vorbereitende Schritte

- Ihre Anmeldeberechtigungsnachweise müssen der Konfigurationsaktion zugeordnet sein.
- Die Verwendung der Einstellung "URL-Präfix" muss mit der browserbasierten Instanz von IBM SPSS Deployment Manager aktiviert werden.

Vorgehensweise

1. Melden Sie sich bei der browserbasierten Instanz von IBM SPSS Deployment Manager.
2. Klicken Sie in der Anzeige **Konfiguration** in der Gruppe **Setup** auf die Option **URL-Präfix**.
3. Fügen Sie der Definition **URL-Präfix** das Kontextstammverzeichnis 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 erneut.

Nächste Schritte

Aktualisieren Sie das Kontextstammverzeichnis für jede Anwendung. Welche Schritte auszuführen sind, hängt vom Anwendungsserver ab.

Zugehörige Konzepte

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

Zugehörige Tasks

Aktualisieren von Kontextstammverzeichnissen für WebSphere
Ändern Sie mithilfe der Administrationskonsole die Position, an der auf Anwendungen zugegriffen wird, die in WebSphere bereitgestellt werden.

Aktualisieren von Kontextstammverzeichnissen für JBoss
Ändern Sie die Position, an der auf Anwendungen zugegriffen wird, die in JBoss bereitgestellt werden, indem Sie die EAR-Datei mit den Positionsdefinitionen aktualisieren.

Aktualisieren von Kontextstammverzeichnissen für WebSphere

Ändern Sie mithilfe der Administrationskonsole die Position, an der auf Anwendungen zugegriffen wird, die in WebSphere bereitgestellt werden.

Vorbereitende Schritte

„Hinzufügen eines Kontextstammverzeichnisses zum URL-Präfix” auf Seite 56

Vorgehensweise

1. Melden Sie sich bei der WebSphere-Konsole an.
2. Greifen Sie auf die Anwendung IBM SPSS Collaboration and Deployment Services zu.
3. Aktualisieren Sie die Einstellungen für das **Kontextstammverzeichnis für Webmodule** so, dass Ihr Stammverzeichniswert eingeschlossen wird.

   Ist das URL-Präfix für Ihr System aktiviert, muss der Stammverzeichniswert für die einzelnen Module mit dem Wert identisch sein, 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 wurde.

Zugehörige Konzepte

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

Zugehörige Tasks

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

Aktualisieren von Kontextstammverzeichnissen für JBoss
Ändern Sie die Position, an der auf Anwendungen zugegriffen wird, die in JBoss bereitgestellt werden, indem Sie die EAR-Datei mit den Positionsdefinitionen aktualisieren.

Aktualisieren von Kontextstammverzeichnissen für JBoss

Ändern Sie die Position, an der auf Anwendungen zugegriffen wird, die in JBoss bereitgestellt werden, indem Sie die EAR-Datei mit den Positionsdefinitionen aktualisieren.

Vorbereitende Schritte

„Hinzufügen eines Kontextstammverzeichnisses zum URL-Präfix” auf Seite 56

Vorgehensweise

1. Erstellen Sie im Verzeichnis `toDeploy/timestamp` Ihrer JBoss-Installation eine Sicherungskopie der `cds83.ear`-Datei.
2. Ändern Sie die Datei `META-INF/application.xml` mithilfe eines Archivierungsdienstprogramms in die ursprüngliche EAR-Datei.

   Stellen Sie den Stammverzeichniswert der Anwendung bei jedem `context-root`-Element mit dem neuen Kontextstammverzeichnis voran. Sie müssen jedem `context-root`-Element den gleichen 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 erneut.

Beispiel

Angenommen, die Datei `application.xml` enthält folgende 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>
```

Wenn Sie ein Kontextstammverzeichnis von `ibm/spss` hinzufügen möchten, aktualisieren Sie die `context-root`-Definitionen mit 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>
```

Zugehörige Konzepte

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

Zugehörige Tasks

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

Aktualisieren von Kontextstammverzeichnissen für WebSphere
Ändern Sie mithilfe der Administrationskonsole die Position, an der auf Anwendungen zugegriffen wird, die in WebSphere bereitgestellt werden.

Kapitel 7. FIPS 140–2-Konformität

Bei dem Federal Information Processing Standard (FIPS), Veröffentlichung 140-2, FIPS PUB 140-2, handelt es sich um einen Computersicherheitsstandard der US-Regierung zur Akkreditierung von Verschlüsselungsmodulen. Das Dokument gibt die Anforderungen für Verschlüsselungsmodule an, zu denen sowohl Hardware- als auch Softwarekomponenten zählen, die vier verschiedenen Sicherheitsstufen entsprechen. Diese sind für Organisationen vorgeschrieben, die Geschäfte mit der US-Regierung machen. IBM SPSS Collaboration and Deployment Services kann so konfiguriert werden, dass Sicherheitsstufe 1 gemäß FIPS 140-2 gewährleistet wird.

Bei der Sicherheitskonfiguration für FIPS 140-2-Konformität sind folgende Richtlinien zu befolgen:

- Bei der Kommunikation zwischen dem Repository und Clientanwendungen muss SSL verwendet werden, damit bei allgemeinen Datenübertragungen Transport Layer Security gewährleistet ist. Für Berechtigungsnachweiskennwörter wird zusätzliche AES-Verschlüsselung geboten. Dabei wird ein gemeinsam genutzter Schlüssel verwendet, der im Anwendungscode gespeichert ist. Weitere Informationen finden Sie im Thema Kapitel 8, „Verwenden von SSL zur sicheren Datenübertragung”, auf Seite 61.
- Der Repository-Server verwendet den AES-Algorithmus mit dem Schlüssel, der in einem Keystore auf dem Serverdateisystem gespeichert ist, um Kennwörter in den Konfigurationsdateien, Konfigurationsdateien für den Anwendungsserver, Konfigurationsdateien für den Sicherheitsprovider usw. zu verschlüsseln.
- Bei der Kommunikation zwischen dem Repository-Server und dem Datenbankserver kann optional SSL für Transport Layer Security verwendet werden, um die allgemeine Datenübertragung zu gewährleisten. Die AES-Verschlüsselung wird für Berechtigungsnachweiskennwörter, Konfigurationskennwörter, Benutzervorgabekennwörter usw. zur Verfügung gestellt. Dabei wird ein gemeinsam genutzter Schlüssel verwendet, der in einem Keystore auf dem Dateisystem des Datenbankservers gespeichert ist.

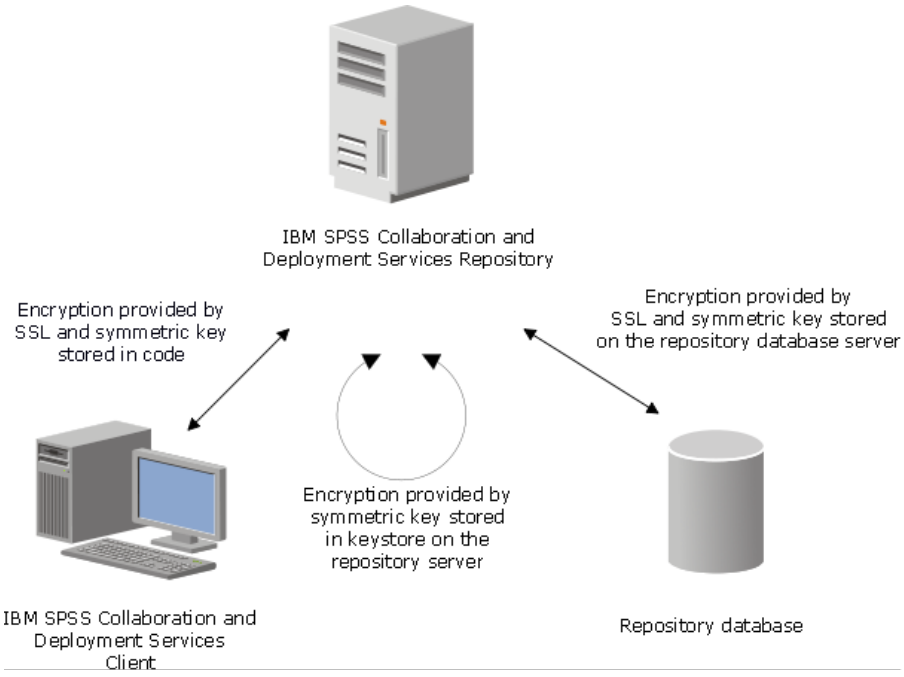

Abbildung 4. IBM SPSS Collaboration and Deployment Services FIPS 140-2-kompatible Sicherheitskonfiguration

Repository-Konfiguration

Bei der Repository-Konfiguration für FIPS 140-2-Konformität sind folgende Richtlinien zu befolgen:

- Die Datenbank muss so eingerichtet werden, dass SSL-Kommunikation akzeptiert wird. Das JCE-Verschlüsselungsmodul muss ebenfalls konfiguriert werden.
- Wenn das Repository unter UNIX installiert wird, muss die Standard-JRE mit einem JCE-Modul eingerichtet werden.
- Die JRE des Anwendungsservers muss ebenfalls mit einem JCE-Modul eingerichtet werden.
- Der Anwendungsserver muss so konfiguriert werden, dass SSL-Kommunikation akzeptiert wird. Das JCE-Verschlüsselungsmodul muss ebenfalls konfiguriert werden.
- Wenn das Repository unter Windows installiert wird, müssen Sie die Installation auf dem Einrichtungsbildschirm beenden, ein JCE-Modul konfigurieren, erneut mit der Einrichtung beginnen und auf dem entsprechenden Bildschirm die Ausführung im FIPS 140-2-kompatiblen Modus auswählen.
- Wenn das Repository in einer Clusterumgebung bereitgestellt wird, muss der Keystore auf allen Knoten im Cluster repliziert werden.
- In den JREs, die von Serveranwendungen von IBM Corp. verwendet werden, die mit IBM SPSS Collaboration and Deployment Services interagieren, wie z. B. IBM SPSS Statistics Server und IBM SPSS Modeler Server, müssen SSL-Zertifikate installiert sein.

Konfiguration des Desktop-Clients

Bei IBM SPSS Collaboration and Deployment Services-Desktop-Clientanwendungen wie der Instanz von IBM SPSS Deployment Manager muss das JCE-Verschlüsselungsmodul aktiviert sein, damit die verwendete JRE die Anwendungen ausführt. In der JRE müssen SSL-Zertifikate installiert sein.

Browserkonfiguration

- Mozilla Firefox kann so konfiguriert werden, dass es im FIPS 140-2-konformen Modus ausgeführt wird, indem die Anwendungsoptionen geändert werden. Weitere Informationen finden Sie in http://support.mozilla.com/en-US/kb/Configuring+Firefox+for+FIPS+140-2.
- Für die Internet Explorer-Konfiguration ist eine Aktivierung der Verschlüsselung von Windows und eine Änderung der Browsereinstellungen erforderlich. Weitere Informationen hierzu finden Sie im Thema http://support.microsoft.com/kb/811833.
- Apple Safari kann im FIPS 140-2-konformen Modus nicht verwendet werden.

Kapitel 8. 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 stellt sicher, 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.

Führen Sie diese allgemeinen Schritte aus, um SSL mit einem unterstützten Anwendungsserver zu verwenden:

1. Importieren Sie das SSL-Zertifikat in die JRE von IBM Installation Manager.
2. Wählen Sie während der Installation die Option **SSL-fähig** aus, um die SSL-Verbindung zur Datenbank zu aktivieren.
3. Importieren Sie nach der Installation und vor dem Serverstart das Zertifikat in die JRE, die in IBM SPSS Collaboration and Deployment Services enthalten ist.

Weitere Anweisungen in Bezug auf Ihren Anwendungsserver finden Sie in „Konfigurieren von SSL für Anwendungsserver” auf Seite 64.

Funktionsweise von SSL

SSL beruht auf dem öffentlichen und privaten Schlüssel des Servers sowie einem Zertifikat für den öffentlichen Schlüssel, 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 Zertifikat für den öffentlichen Schlüssel.
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 Zertifikat für den öffentlichen Schlüssel ist in der Regel von einer Zertifizierungsstelle signiert. Zertifizierungsstellen wie VeriSign und Thawte sind Organisationen, die Sicherheitsdaten, die sich in den Zertifikaten für öffentliche Schlüssel 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 selbst signierte Zertifikate generiert werden.

IBM SPSS Statistics Server unterstützt sowohl OpenSSL als auch GSKit. Wenn beide konfiguriert sind, 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. Wenn Sie Verschlüsselungszertifikate verwenden, die eine Verschlüsselung mit einer Stärke von über 2048 Bit aufweisen, installieren Sie Verschlüsselung mit unbegrenzter Stärke auf den Deployment Manager-Client-Computern. Weitere Information finden Sie in „Installieren der Verschlüsselung mit unbegrenzter Stärke” auf Seite 62
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: Außerdem müssen Sie die Dateien mit der Erweiterung `*.jar` im Ordner `<Deployment_Manager-Client-Installation>/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 in der Liste unter **Sicherheit > Sichere Verwaltung, Anwendungen und Infrastruktur** auswählen und dann auf **Als aktuell festlegen** klicken müssen, damit 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*. Dabei ist *<installationsordner>* der Ordner, 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 über SSL eine Verbindung zu einem IBM SPSS Collaboration and Deployment Services-Repository und Sie selbst signierte Zertifikate verwenden, müssen Sie das Zertifikat dem Java-Keystore des Clients hinzufügen. Folgende Schritte werden auf dem *Client-Computer* ausgeführt.

1. Öffnen Sie eine Eingabeaufforderung und ändern Sie Verzeichnisse in die folgende Position. Dabei steht *<Produktinstallationsverzeichnis>* für das Verzeichnis, in dem Sie das Produkt installiert haben:

   ```
   <Produktinstallationsverzeichnis>/jre/bin
   ```

2. Geben Sie folgenden Befehl ein:

```
keytool -import -alias <Aliasname> -file <Zertifikatspfad> -keystore <key
store-Pfad>
```

   Dabei steht *<Aliasname>* für einen beliebigen Alias für das Zertifikat, *<Zertifikatspfad>* für den vollständigen Pfad zum Zertifikat und *<Keystore-Pfad>* für den vollständigen Pfad zum Java-Keystore (z. B *<Produktinstallationsverzeichnis>/lib/security/jssecacerts* oder *<Produktinstallationsverzeichnis>/lib/security/cacerts*).

3. Geben Sie bei entsprechender Aufforderung das Keystore-Kennwort ein, das standardmäßig `changeit` lautet.
4. Wenn Sie gefragt werden, ob Sie dem Zertifikat vertrauen, geben Sie `ja` ein.

Importieren der Zertifikatsdatei für Verbindungen zu einem browserbasierten Client

Wenn Sie mit einem browserbasierten Client (z. B. IBM SPSS Collaboration and Deployment Services Deployment Portal) über SSL eine Verbindung zu IBM SPSS Collaboration and Deployment Services Repository herstellen, fordert der Browser Sie dazu auf, das nicht signierte, nicht vertrauenswürdige Zertifikat zu akzeptieren. Alternativ wird im Browser eine Nachricht angezeigt, in der darauf hingewiesen wird, dass die Site nicht sicher ist, und ein Link bereitgestellt, über den das Zertifikat in den Browser-Truststore importiert werden kann. Dieser Prozess unterscheidet sich von anderen Browsern und kann je nach Browserkonfiguration variieren. Sie können das Zertifikat auch manuell im Browser-Truststore installieren.

Anweisung an Benutzer, SSL zu aktivieren

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

Konfigurieren des URL-Präfix

Wenn IBM SPSS Collaboration and Deployment Services Repository für SSL-Zugriff eingerichtet ist, muss die Konfigurationseinstellung für das URL-Präfix wie folgt geändert werden:

1. Melden Sie sich über die browserbasierte Konsole am Repository an.
2. Öffnen Sie die Konfigurationsoption *URL-Präfix*.

   Konfiguration > **Setup** > **URL-Präfix**

3. Setzen Sie den Wert des Präfix auf `https` anstelle von `http` und setzen Sie den Portwert auf die SSL-Portnummer. Beispiel:

```
[default]
http://<hostname>:<port>
[SSL-enabled]
https://<hostname>:<SSLport>
```

Schützen von LDAP durch SSL

LDAP (Lightweight Directory Access Protocol) ist ein IETF-Standard (IETF - Internet Engineering Task Force) für den Austausch von Informationen zwischen Netzverzeichnissen und -datenbanken mit einer beliebigen Informationsstufe. Bei Systemen, die zusätzliche Sicherheit erfordern, können LDAP-Provider wie Microsofts Active Directory über SSL (Secure Socket Layer) betrieben werden, vorausgesetzt, das Web oder der Anwendungsserver unterstützt LDAP über SSL. Die Verwendung von SSL zusammen mit LDAP kann sicherstellen, dass Anmeldekennwörter, Anwendungsinformationen und andere vertrauliche Daten nicht entwendet, beeinträchtigt oder gestohlen werden.

Das folgende Beispiel veranschaulicht die Aktivierung von LDAPS mithilfe von Microsofts Active Directory als Sicherheitsprovider. Genauere Informationen zu einzelnen Schritten oder Details für ein bestimmtes Release des Sicherheitsproviders finden Sie in der Originaldokumentation des Herstellers.

1. Prüfen Sie, ob Active Directory und die Unternehmenszertifizierungsstelle installiert sind und funktionieren.
2. Generieren Sie mithilfe der Zertifizierungsstelle ein Zertifikat und importieren Sie es in den Zertifikatsspeicher der Installation von IBM SPSS Deployment Manager. Hierdurch kann die LDAPS-Verbindung zwischen IBM SPSS Collaboration and Deployment Services Repository und einem Active Directory-Server hergestellt werden.

   Stellen Sie sicher, dass eine Verbindung zum Repository vorhanden ist, um IBM SPSS Deployment Manager für sichere Active Directory-Verbindungen konfigurieren zu können.
3. Starten Sie IBM SPSS Deployment Manager.
4. Wählen Sie im Menü **Tools** die Option **Serveradministration** aus.
5. Melden Sie sich an einem zuvor definierten verwalteten Server an.
6. Doppelklicken Sie auf das Symbol **Konfiguration** für den Server, um die Hierarchie einzublenden.
7. Doppelklicken Sie auf das Symbol **Sicherheitsprovider**, um die Hierarchie einzublenden.
8. Doppelklicken Sie auf den Sicherheitsprovider Active Directory.
9. Geben Sie Konfigurationswerte für die Instanz von Active Directory bei installierten Sicherheitszertifikaten ein.
10. Wählen Sie das Kontrollkästchen **SSL verwenden** aus.
11. Notieren Sie den Namen im Feld **Domänenbenutzer**. Nachfolgende Anmeldungen über Active Directory werden mithilfe von SSL authentifiziert.

Weitere Informationen zum Installieren, Konfigurieren und Implementieren von LDAPS auf einem bestimmten Anwendungsserver finden Sie in der Originaldokumentation des Herstellers.

Konfigurieren von SSL für Anwendungsserver

Sie können IBM SPSS Collaboration and Deployment Services Repository Server für eine SSL-fähige Datenbank installieren. Führen Sie für Ihren Anwendungsserver die folgenden Schritte aus:

JBoss

Anweisungen zum Aktivieren von SSL/TLS finden Sie in der Dokumentation zu JBoss EAP 7.x. SSL ist in JBoss EAP 7.x standardmäßig aktiviert. Nehmen Sie folgende Anpassungen vor:

1. Erstellen Sie eine Schlüsseldatei im Java-Keystore-Format. Beispiel:

   ```
   keytool -genkey -alias cads822  -keyalg RSA -ext san=ip:*.**.**.**  -keystore myserver.jks -
   validity 10950
   ```

   Stellen Sie sicher, dass der allgemeine Name (CN) dem vollständig qualifizierten Domänennamen (FQDN) des Systems entspricht, auf dem IBM SPSS Collaboration and Deployment Services Repository installiert ist. `ip` entspricht der IP-Adresse von IBM SPSS Collaboration and Deployment Services Repository Server.

   Wenn die Schlüsseldatei nicht im Keystoreformat vorliegt, konvertieren Sie sie zuerst in das Java-Keystore-Format.
2. Aktualisieren Sie die folgenden SSL-Einstellungen in der Datei `cds_server.xml` in `JBOSS_HOME\standalone\configuration`:

   ```
   <security-realm name="CaDSRealm">
   <server-identities>
   <ssl>
   <keystore path="JBOSS_HOME\standalone\configuration\myserver.jks" keystore-password="xxxx"
   alias="cads822"/>
   </ssl>
   ```

```
...
</security-realm>
```

Hierbei entspricht der Wert für `alias` dem Namen, den Sie zum Erstellen der Schlüsseldatei verwendet haben.

```
<http-connector name="http-remoting-connector" connector-ref="default" security-realm="CaDS
Realm"/>
```

```
<https-listener name="https" socket-binding="https" security-realm="CaDSRealm" enable-
http2="true"/>
```

3. Optional: Sie können Änderungen an der Portkonfiguration vornehmen. Ändern Sie z. B. den Standard-HTTPS-Port für JBoss von 8443 in 443 unter `<socket-binding-group>` in der Datei `cds_server.xml`:

```
<socket-binding-group name="standard-sockets" default-interface="public" ...>
<socket-binding name="http" port="80" />
<socket-binding name="https" port="443" />
...
</socket-binding-group>
```

Liberty

Anweisungen zum Aktivieren von SSL/TLS finden Sie in der Dokumentation zu JBoss EAP 7.x. SSL ist in JBoss EAP 7.x standardmäßig aktiviert. Nehmen Sie folgende Anpassungen vor:

1. Erstellen Sie eine Schlüsseldatei im Java-Keystore-Format. Beispiel:

```
keytool -genkey -alias test.jks -keyalg RSA san=ip:*.**.**.**  -validity 20000 -keystore
test.jks
```

Stellen Sie sicher, dass der allgemeine Name (CN) dem vollständig qualifizierten Domänennamen (FQDN) des Systems entspricht, auf dem IBM SPSS Collaboration and Deployment Services Repository installiert ist. `ip` entspricht der IP-Adresse von IBM SPSS Collaboration and Deployment Services Repository Server.

Wenn die Schlüsseldatei nicht im Keystoreformat vorliegt, konvertieren Sie sie zuerst in das Java-Keystore-Format.

2. Aktualisieren Sie die Datei `server.xml` in `CADS_HOME\wlp\usr\servers\cdsServer` mit den Informationen der neuen Keystore-Datei:

```
<keyStore id="defaultKeyStore" location=".\test.jks" type="JKS" password="xxxx"/>
```

WebSphere

Anweisungen zum Aktivieren von SSL/TLS finden Sie in der Dokumentation zu WebSphere.

Kapitel 9. 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 2-Paket zur Handhabung der Informationen aus dem Laufzeitprotokoll. Log4j 2 ist die Protokolllösung der Apache Software Foundation für Java-Anwendungen. Die Methode log4j 2 ermöglicht die Steuerung der Protokollierung über eine Konfigurationsdatei; die Binärdatei der Anwendung muss dabei nicht verändert werden. Umfangreiche Informationen zu log4j 2 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/log4j2.xml`
- **Liberty:** `<Repository-Installationsverzeichnis>/platform/log4j2.xml`
- **JBoss:** `<JBoss-Serververzeichnis>/standalone/configuration/log4j2.xml`

In dieser Datei sind sowohl der Speicherort als auch der Umfang der Protokollausgabe festgelegt. Die Konfiguration von log4j 2 wird über eine Anpassung dieser Datei vorgenommen, bei der Appender für das Protokollziel definiert werden und die Ausgabe der Protokollfunktion an diese Appender geleitet wird.

Folgende Standardprotokollfunktionen sind definiert:

Tabelle 4. 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*)
- Export-Import-Transaktionsprotokoll (*cds_transfer.log*)

Der Standardspeicherort der Protokolldateien variiert abhängig vom Hostanwendungsserver:

- **WebSphere:** <WebSphere-Profilverzeichnis>/logs/
- **JBoss:** <JBossSerververzeichnis>/standalone/log
- **Liberty:** <Repository-Installationsverzeichnis>/wlp/usr/servers/cdsServer/logs

Kapitel 10. Beispiel: WebSphere-Clusterinstallation und -Konfiguration

Dieser Abschnitt enthält ein End-to-End-Beispiel für die Installation und Konfiguration des IBM SPSS Collaboration and Deployment Services Repositorys mit einem IBM WebSphere-Cluster-Server.

Dieses Beispiel umfasst folgende Informationen:

- Die Schritte zur **Vorinstallation** für die Ermittlung der Systemanforderungen basierend auf Ihrem Installationstyp und der Systemverwendung, für die Bereitstellung der Systeme, auf denen der Cluster von Anwendungsservern ausgeführt werden soll, und für die Sicherstellung, dass die Server alle Hardware- und Softwareanforderungen erfüllen.
- Die Schritte des **WebSphere-Cluster-Servers** für die Installation von WebSphere mit IBM Installation Manager und die Einrichtung eines WebSphere-Cluster-Servers.
- Die Schritte im Bereich der **Datenbank** für die Initialisierung Ihrer Datenbank.
- Die Schritte zur **Installation und Konfiguration** für die Installation der Anwendungsdateien auf dem Hostsystem mit IBM Installation Manager und die Konfiguration des IBM SPSS Collaboration and Deployment Services Repositorys zur Ausführung des Repositorys mit dem festgelegten Cluster von Anwendungsservern und der Repository-Datenbank.
- Die Schritte **nach der Installation** für das Starten des IBM SPSS Collaboration and Deployment Services Repositorys und das Prüfen der Konnektivität.

Installationsvorbereitung

Bevor Sie IBM SPSS Collaboration and Deployment Services mit einem WebSphere-Cluster-Server installieren, sollten Sie prüfen, ob Ihre Umgebung auf sämtlichen Knoten des Clusters alle Hardware- und Softwareanforderungen erfüllt. Weitere Informationen finden Sie in den Berichten zur Kompatibilität von IBM Softwareprodukten unter:https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html

Bei der Bereitstellung des IBM SPSS Collaboration and Deployment Services Repository-Servers in einer Umgebung mit Clusteranwendungsserver muss jeder Anwendungsserver im Cluster eine identische Konfiguration für die gehosteten Anwendungskomponenten aufweisen. Ferner sollte der Zugriff auf das Repository über eine hardware- oder softwarebasierte Lastausgleichsfunktion erfolgen. Durch diese Architektur wird eine Verteilung der Verarbeitung über mehrere Anwendungsserver ermöglicht. Zudem bietet sie Redundanz im Falle eines Serverfehlers.

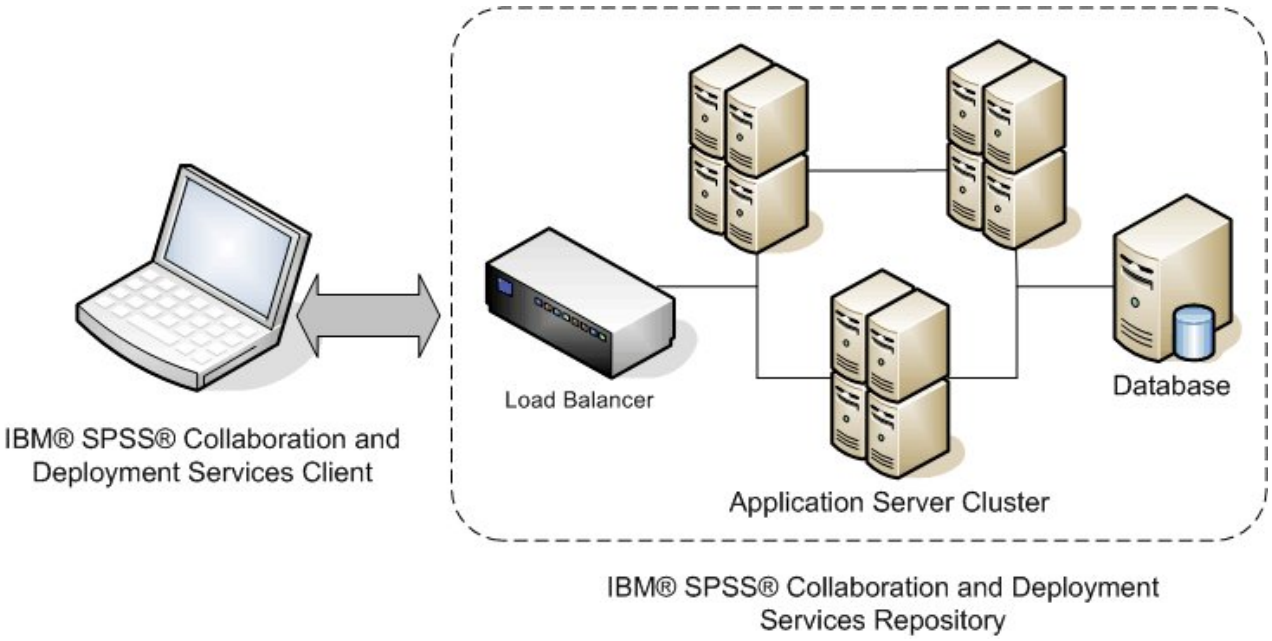

Abbildung 5. Clusterarchitektur

Die Installation des Repository-Servers in einem Cluster umfasst die folgenden Schritte:

- Erstinstallation und -konfiguration der Anwendungskomponenten auf dem Managementknoten des Clusters
- Anschließende Konfiguration der Clusterknoten

Installationsvoraussetzungen

- Die Hostsystemanforderungen müssen auf allen Knoten des Clusters erfüllt sein.
- Alle Clustermember müssen unter demselben Betriebssystem als Hauptknoten (Managementknoten) ausgeführt werden.
- Die IBM SPSS Collaboration and Deployment Services Repository-Datenbank muss bereits vor der Installation des Repositorys vorhanden und zugänglich sein.
- Die Topologie des Anwendungsservers muss bereits vor der Installation des Repositorys vorhanden sein. Wir empfehlen zu prüfen, ob der Cluster zugänglich ist und an der Adresse der Lastausgleichsfunktion ordnungsgemäß ausgeführt wird.
- Das Repository-Installationsverzeichnis muss im Cluster knotenübergreifend gemeinsam genutzt werden.

Installation des WebSphere-Cluster-Servers

Vor der Installation von IBM WebSphere muss IBM Installation Manager 1.9.1 oder höher installiert werden. Weitere Informationen zur Installation von IBM Installation Manager finden Sie unter https://jazz.net/wiki/bin/view/Deployment/InstallingUpdatingScriptingWithInstallationManager.

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

Installation 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 Installationsdateien von IBM WebSphere Application Server 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 Sprachen aus, in denen übersetzte Inhalte installiert werden sollen, und klicken Sie auf **Weiter**.
8. Wählen Sie die Funktionen aus, die installiert werden sollen, und klicken Sie auf **Weiter**.
9. Prüfen Sie die Übersichtsinformationen und klicken Sie auf **Installieren**.

Wichtig: WebSphere Application Server müsste auf allen Knoten in der entworfenen WebSphere-Clustertopologie installiert sein. Wiederholen Sie die vorherigen Schritte auf allen Knoten im Cluster.

Einrichtung des Cluster-Servers

Stellen Sie vor der Einrichtung eines Cluster-Servers sicher, dass das WebSphere-Profil, das mit IBM SPSS Collaboration and Deployment Services verwendet wird, für die Ausführung mit dem Java SDK 7 oder höher konfiguriert ist. Das folgende Beispiel zeigt die Befehlsfolge zur Auflistung verfügbarer DKs sowie zum Festlegen von standardmäßigen SDKs.

```
<WebSphere-Installationsverzeichnis> \bin>managesdk.bat –listAvailable
CWSDK1003I: Available SDKs :
CWSDK1005I: SDK name: 8.0_64
CWSDK1001I: Successfully performed the requested managesdk task.
<WebSphere-Installationsverzeichnis>\bin>managesdk.bat -setNewProfileDefault -sdkName 8.0_64
CWSDK1022I: New profile creation will now use SDK name 8.0_64.
CWSDK1001I: Successfully performed the requested managesdk task
```

Wichtig: Stellen Sie sicher, dass sich auf allen Knoten im Cluster das Java SDK der Version 7 oder höher befindet.

Eine Clustertopologie enthält in der Regel einen Managementknoten und einige verwaltete Knoten. WebSphere bietet ein Dienstprogramm für die Profilverwaltung, das für die Erstellung von Profilen verwendet werden kann. Beispiel:

1. Erstellen Sie das Profil *Bereitstellungsmanagement* auf dem *Managementsystem*:
   - Melden Sie sich bei dem *Managementknoten* an und führen Sie das Dienstprogramm für die Profilverwaltung aus. Beispiel:
     – Windows:

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

     – Linux/UNIX:

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

2. Erstellen Sie das Profil *Bereitstellungsmanagement* auf dem *verwalteten System*:
   - Melden Sie sich bei dem *verwalteten* Knoten an und führen Sie das Dienstprogramm für die Profilverwaltung aus. Beispiel:
     – Windows:

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

     – Linux/UNIX:

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

     Wichtig: Wenn in Ihrer Clustertopologie zwei oder mehr verwaltete Knoten vorhanden sind, führen Sie diesen Befehl mehrmals aus, um auf jedem verwalteten System verwaltete Profile 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 System befindet als ein Managementprofil, sollten Sie sicherstellen, dass die Netzkonnektivität zwischen dem Managementprofil und dem verwalteten System ordnungsgemäß funktioniert.

1. Starten Sie das *Managementprofil* auf dem *Managementknoten*:
   - Melden Sie sich bei dem *Managementsystem* 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* die *verwalteten* Knoten hinzu:
   - Melden Sie sich bei dem *verwalteten* System 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 steht `<Management-Host>` für den Hostnamen des Managementsystems. `Port` steht für den Management-SOAP-Connector-Port des Managementprofils, der in der Datei `AboutThisProfile.txt` zu finden ist. Wenn in Ihrer Clustertopologie zwei oder mehr verwaltete Knoten vorhanden sind, führen Sie diesen Befehl mehrmals für jedes Profils aus.
3. Melden Sie sich bei der WebSphere-Administrationskonsole an und erstellen Sie basierend auf den verwalteten Knoten eine Clusterdefinition:
   - Melden Sie sich bei der WebSphere-Administrationskonsole des Managementprofils an (`https://hostname:port/ibm/console/logon.jsp`, wobei `hostname` für den Hostnamen des Managementsystems und `port` für die Portnummer der Administrationskonsole steht).
   - 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 für den ersten Cluster-Member einen Membernamen an und wählen Sie einen der verfügbaren Knoten aus. Klicken Sie auf **Weiter**.
- Erstellen Sie zusätzliche Cluster-Member, indem Sie andere verfügbare Knoten hinzufügen.

Datenbank

Die Datenbank und das IBM SPSS Collaboration and Deployment Services Repository müssen nicht auf demselben Server installiert werden, jedoch sind einige Konfigurationsschritte erforderlich, um die Konnektivität sicherzustellen. Während der Installation werden Sie zur Eingabe des Namens des Datenbankservers, der Portnummer, des Benutzernamens mit dem zugehörigen Kennwort und des Namens der Datenbank aufgefordert, die zum Speichern und Abrufen von Informationen verwendet werden soll.

Wichtig: Sie müssen die Datenbank vor der Installation manuell erstellen. Es kann ein beliebiger gültiger Datenbankname verwendet werden. Wenn eine zuvor erstellte Datenbank nicht vorhanden ist, wird die Installation jedoch nicht fortgesetzt.

Im Folgenden finden Sie ein SQL-Beispielscript für die Erstellung einer Db2-Datenbank mit dem Namen 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 BUF
FERPOOL "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 IBM SPSS Collaboration and Deployment Services Repository-Server auf einem WebSphere-Cluster-Server bereitstellen, müssen Sie sicherstellen, dass der Repository-Server auf demselben System installiert wird wie das WebSphere-Managementprofil.

1. Melden Sie sich als Benutzer mit der entsprechenden Berechtigungsstufe beim Betriebssystem an.
2. Öffnen Sie mit einer der folgenden Methoden IBM Installation Manager:
   - GUI-Modus: `<IBM Installation Manager-Installationsverzeichnis>/eclipse/IBMIM`
   - Befehlszeilenmodus: `<IBM Installation Manager-Installationsverzeichnis>/eclipse/tools/imcl -c`
3. Geben Sie den Repository-Pfad an (z. B. in Form einer Position auf dem Hostdateisystem, des Netzes oder einer HTTP-Adresse), wenn das Installationsrepository nicht konfiguriert ist.

   Anmerkung: Damit Sie erfolgreich auf ein Installationsrepository zugreifen können, darf der Pfad zur Repository-Position kein Et-Zeichen (&) enthalten.
4. Wählen Sie im Hauptmenü **Installieren** aus.
5. Wählen Sie IBM SPSS Collaboration and Deployment Services als Paket aus, das installiert werden soll. 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 IBM SPSS Collaboration and Deployment Services Repository-Installation ist eine neue Paketgruppe erforderlich.

- Geben Sie das Installationsverzeichnis für gemeinsam genutzte Ressourcen an. Sie können das Verzeichnis für gemeinsam genutzte Ressourcen nur bei der Erstinstallation eines Pakets angeben.

8. Prüfen Sie die Übersichtsinformationen und fahren Sie mit der Installation fort. Die Anwendungsdateien werde im angegebenen Verzeichnis installiert, nachdem Sie auf **Installieren** geklickt haben.
9. Konfigurieren Sie das freizugebende Installationsverzeichnis so, dass alle Mitglieder im Cluster darauf zugreifen können (verwenden Sie z. B. die Dateifreigabe unter Windows oder NFS unter Linux/UNIX).

   Treten während der Installation Probleme auf, können Sie die Protokolle von IBM Installation Manager zur Fehlerbehebung verwenden. Greifen Sie über das Hauptmenü in IBM Installation Manager auf die Protokolldateien zu.

Konfiguration

Nach der Ausführung der vorherigen Installationsschritte müssten die Situation nun wie folgt aussehen:

- Alle Member im WebSphere-Cluster werden auf demselben Betriebssystem ausgeführt wie der Hauptknoten (Managementknoten)
- Die Repository-Datenbank ist vorhanden und zugänglich
- Das IBM SPSS Collaboration and Deployment Services Repository-Installationsverzeichnis wurde für alle Knoten in Ihrem WebSphere-Cluster freigegeben

Repository-Server in Ihrem Cluster bereitstellen

1. Starten Sie mit einer der folgenden Methoden das Konfigurationsdienstprogramm:
   - 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 den Typ **IBM WebSphere** aus.
3. Geben Sie Anwendungsservereinstellungen wie folgt an:
   - **WebSphere-Profilverzeichnis.** Die Verzeichnisposition des WebSphere-Serverprofils. Bei einem WebSphere-Cluster ist dies der Pfad des Managementprofils. Andere WebSphere-Einstellungen, wie z. B. WebSphere-Installationsstammverzeichnis, Profiltopologie und Knoten, werden automatisch basierend auf den Profilinformationen gefüllt. Wenn Werte nicht automatisch gefüllt werden können, müssen Sie diese manuell angeben.
   - **URL-Präfix.** Die URL, die für den Zugriff auf den Repository-Server verwendet wird (z. B. `http://<System>:<Port>`). In einer Clusterumgebung stellt der Port in der Regel die Portnummer der Lastausgleichsfunktion dar.
4. Geben Sie die Datenbankverbindungsinformationen wie folgt an:
   - **Datenbanktyp.** IBM Db2, SQL Server oder Oracle.
   - **Host.** Der Hostname oder die IP-Adresse des Datenbankservers.
   - **Port.** Der Zugriffsport für den Datenbankserver.
   - **Datenbankname.** Der Name der Datenbank, die für das Repository verwendet werden soll.
   - **Quellen-ID/Servicename.** Bei Oracle die Quellen-ID oder der Servicename.
   - **Als Service ausführen.** Gibt bei Oracle an, dass die Verbindung zu einem Datenbankservice besteht und nicht über die Quellen-ID hergestellt wurde.
   - **Benutzername.** Der Datenbankbenutzername.
   - **Kennwort.** Das Kennwort des Datenbankbenutzers.

5. Geben Sie bei der Wiederverwendung 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. Bei dem Keystore handelt es sich um eine verschlüsselte Datei, die den Schlüssel zum Entschlüsseln der Kennwörter enthält, die vom Repository verwendet werden (z. B. das Kennwort für die Repository-Verwaltung, das Kennwort für den Datenbankzugriff usw.).
   - Geben Sie zur Wiederverwendung eines Keystores aus einer vorhandenen Repository-Installation den Pfad und das Kennwort für den Keystore an. Der Schlüssel aus dem alten Keystore wird extrahiert und im neuen Keystore verwendet. Beachten Sie, dass die JRE, die zur Ausführung des Anwendungsservers verwendet wird, mit der JRE kompatibel sein muss, die zum Erstellen der Verschlüsselungsschlüssel verwendet wurde.
   - Wenn Sie einen vorhandenen Keystore nicht wiederverwenden, geben Sie das Kennwort für den neuen Keystore an und bestätigen Sie dieses. Der Keystore wird unter `<Repository-Installationsverzeichnis>/keystore` erstellt.

   Wichtig: Wenn Sie die Keystore-Datei verlieren, ist die Anwendung nicht in der Lage, Kennwörter zu entschlüsseln, und kann nicht mehr verwendet werden. Sie muss folglich erneut installiert werden. Wir empfehlen Ihnen, Sicherungskopien der Keystore-Datei zu speichern.
7. Geben Sie den Kennwortwert an, der für das Benutzerkonto des Administrators (`admin`) für das integrierte Repository verwendet werden soll. Dieses Kennwort wird bei der ersten Anmeldung beim Repository verwendet.
8. Wählen Sie den Bereitstellungsmodus (automatisch oder manuell) aus. In diesem Beispiel wählen wir **automatisch** aus.
9. Prüfen Sie die Übersichtsinformationen und fahren Sie mit der Konfiguration fort.

Cluster konfigurieren

Wenn der IBM SPSS Collaboration and Deployment Services Repository-Server erfolgreich in Ihrem WebSphere-Cluster bereitgestellt wurde, müssen einige externe Konfigurationsschritte ausgeführt werden, damit sichergestellt ist, dass der Server für jeden Knoten im Cluster oder über die Lastausgleichsfunktion zugänglich ist.

1. Legen Sie für jeden Knoten die Variable `CDS_HOME` fest:
   - Melden Sie sich bei der WebSphere-Administrationskonsole an.
   - Gehen Sie zu **Umgebung** > **WebSphere-Variablen**
   - Prüfen Sie bei jedem Knoten den Wert der Variable **CDS_HOME**. Wenn sich ein WebSphere-Knoten auf einem anderen Server als dem Repository-Server befindet, aktualisieren Sie den Wert der Variable CDS_HOME so, dass er auf das gemeinsam genutzte Installationsverzeichnis verweist (z. B. `\\<Management-Host>\SPSS\Deployment\8.2\Server`, wobei `<Management-Host>` für den Hostnamen des Systems steht, auf dem der Repository-Server installiert ist.
2. Legen Sie für jeden Knoten `Log4j-Eigenschaften` fest:
   - Melden Sie sich bei der WebSphere-Administrationskonsole an.
   - Suchen Sie unter **Server** > **WebSphere Application Server** > **[Servername]** > **Java und Prozessmanagement** > **Prozessdefinition** > **Java Virtual Machine** > **Benutzerdefinierte Eigenschaften** nach `log4j.cnfigurationFile`. Diese Eigenschaft gibt die Position an, an der das Protokollierungssystem auf die Konfigurationsdatei für die Protokollierung zugreifen kann. Normalerweise hat diese Eigenschaft den Wert `file://${CDS_HOME}/platform/log4j2.xml`.Enthält die Variable `CDS_HOME` unter Windows einen Laufwerkbuchstaben, fügen Sie dem Wert `log4j.configurationFile` als Escapezeichen einen Schrägstrich hinzu (z. B. `file:///${CDS_HOME}/platform/log4j2.xml`).
   - 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 Application Server enthalten integrierte Dienstprogramme mit einer softwarebasierten Lastausgleichsfunktion (zum Beispiel IBM HTTP Server). In den folgenden Schritten wird die Vorgehensweise bei der Installation und Konfiguration eines IBM HTTP Server beschrieben.

IBM HTTP Server installieren

1. Starten Sie IBM Installation Manager
2. Konfigurieren Sie Installation Manager für die Verwendung eines Repositorys, das 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 für WebSphere Application Server
   - Web-Server-Plug-ins für 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 Funktionen aus, die installiert werden sollen, und klicken Sie auf **Weiter**.
8. Konfigurieren Sie die Details für IBM HTTP Server.
9. Prüfen Sie die Übersichtsinformationen und klicken Sie auf **Installieren**.

Web-Server-Definition in Ihrem WebSphere-Cluster erstellen

1. Melden Sie sich bei der WebSphere-Administrationskonsole des Managementprofils unter `https://hostname:port/ibm/console/logon.jsp` an, wobei `hostname` für den Hostnamen des Managementsystems und `port` für die Portnummer der Administrationskonsole steht.
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 möchten. In der Regel müsste sich der Knoten auf demselben Server befinden, auf dem der HTTP-Server installiert ist. Wählen Sie bei "Typ" die Option **IBM HTTP Server** aus und klicken Sie auf **Weiter**.
4. Wählen Sie die Vorlage aus, die dem Server entspricht, den Sie erstellen möchten, und klicken Sie auf **Weiter**. In diesem Beispiel verwenden wir den Standardwert.
5. Geben Sie Eigenschaften für den neuen Web-Server an.
6. Prüfen Sie die Übersicht der neuen Web-Server-Definition und klicken Sie auf **Fertigstellen**.
7. Speichern Sie Ihre Änderungen.

Web-Server konfigurieren

1. Melden Sie sich bei der WebSphere-Administrationskonsole des Managementprofils an.
2. Suchen Sie unter **Server** > **Servertypen** > **Web-Server** > **[Servername]** nach der Datei `conf.httpd`. Fügen Sie der Datei folgendes Script hinzu:

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

   Dabei steht `<Plug-In-Verzeichnis>` für das Installationsverzeichnis von Web-Server-Plug-ins und `<Web-Server-Name>` für den Namen 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 zu übertragen.

5. Gehen Sie zu **Server** > **Servertypen** > **Web-Server** > **[Servername]** und zeigen Sie `plugin-cfg.xml` an, um sicherzustellen, dass alle URIs für IBM SPSS Collaboration and Deployment Services generiert wurden (z. B. `<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/admin/*"/>`).

Eigenschaft "URL-Präfix" einrichten

In einer Clusterumgebung wird die Eigenschaft **URL-Präfix** für die Repository-Konfiguration für die Weiterleitung der vom Server initiierten HTTP-Anforderungen verwendet. Die Eigenschaft muss auf die URL der Lastausgleichsfunktion festgelegt werden. Beachten Sie, dass Sie diese Eigenschaft bei der erstmaligen Ausführung des IBM SPSS Collaboration and Deployment Services Repository-Konfigurationsdienstprogramms festlegen können.

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

1. Starten Sie einen einzelnen Cluster-Member.
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 bei der Repository-Konfiguration erstellt wurde.
3. Aktualisieren Sie die Konfigurationseigenschaft **URL-Präfix** 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 (entsprechende Anweisungen finden Sie unter diesem Abschnitt).
2. Installieren Sie Inhaltsadapter, die Sie für die Verwendung des IBM SPSS Collaboration and Deployment Services Repositorys mit anderen SPSS-Produkten benötigen, wie z. B. IBM SPSS Modeler oder IBM SPSS Statistics.
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 IBM SPSS Collaboration and Deployment Services-Clients, einschließlich IBM SPSS Deployment Manager. Weitere Informationen finden Sie in den Installationsanweisungen zur Clientanwendung.
5. Erstellen Sie mithilfe von IBM SPSS Deployment Manager Repository-Benutzer und -Gruppen und weisen Sie ihnen über Rollen Anwendungsberechtigungen zu. Weitere Informationen finden Sie im *IBM SPSS Collaboration and Deployment ServicesAdministratorhandbuch*.

Sollten in diesen Schritten nach der Installation Probleme auftreten, finden Sie weitere Informationen im *IBM SPSS Collaboration and Deployment ServicesHandbuch zur Fehlerbehebung*.

Repository-Server starten

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

1. Melden Sie sich beim Managementsystem 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 bei den einzelnen Systemen an und starten Sie die jeweiligen 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 bei der WebSphere-Administrationskonsole des Managementknotens an (http://hostname:port/ibm/console). Gehen Sie zu **Server** > **Servertypen** > **WebSphere Application Server**, wählen Sie die einzelnen Knoten aus und klicken Sie auf **Start**.
4. Gehen Sie zu **Server** > **Servertypen** > **Web-Server** und klicken Sie auf **Start**.

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).

Konnektivität prüfen

Sie können prüfen, ob der IBM SPSS Collaboration and Deployment Services Repository-Server ausgeführt wird, indem Sie über einen unterstützten Web-Browser unter http://<Repository-Host>:<Portnummer>/security/login auf die browserbasierte Instanz von IBM SPSS Deployment Manager zugreifen. Wenn das Tool nicht gestartet wird, wird der Server vermutlich nicht ausgeführt. Weitere Informationen zu unterstützten Web-Browsern finden Sie in den Berichten zur Kompatibilität von IBM Softwareprodukten 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 Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

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

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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 Geschäftsbedingun-

gen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

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

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

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

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

COPYRIGHTLIZENZ:

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

Hinweise zur Datenschutzrichtlinie

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

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

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

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

Marken

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

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

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

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

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

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

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

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

Index

Numerische Stichwörter

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

U

V

W

Z